Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Unidade Acadêmica de Matemática
Curso de Graduação em Matemática

Grupos Aditivos e Multiplicativos de Anéis e Corpos

por

Felipe Barbosa Cavalcante

sob orientação de

Prof. Dr. Antônio Pereira Brandão Júnior

Campina Grande - PB
agosto, 2015

Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Unidade Acadêmica de Matemática
Curso de Graduação em Matemática

Felipe Barbosa Cavalcante

Grupos Aditivos e Multiplicativos de Anéis e Corpos

Trabalho apresentado ao Curso de Graduação em Matemática da Universidade Federal de Campina Grande como requisito para a obtenção do título de Bacharel em matemática.

Orientador: Prof. Dr. Antônio Pereira Brandão Júnior

Campina Grande - PB, agosto de 2015
Curso de Matemática, modalidade Bacharelado

Grupos Aditivos e Multiplicativos de Anéis e Corpos

Felipe Barbosa Cavalcante

Trabalho de conclusão de curso defendido e aprovado em 06 de agosto de 2015, pela Comissão Examinadora constituída pelos professores:

Prof. Dr. Antônio Pereira Brandão Júnior
Orientador

Prof. Dr. Braulio Maia Junior
Examinador

com nota igual a:

Dedicatória

A minha família Sabrina, Saphira, Josefa e Luis.

Agradecimentos

Agradeço inicialmente a minha família: aos meus pais Josefa e Luis pelo suporte durante os estudos e por tantos sacrifícios feitos; a minha esposa Sabrina pelo constante incentivo, apoio, pensamento positivo e todo o companheirismo ofertados durante toda a graduação; a minha filha Saphira por servir de fonte de inspiração e estímulo.

Também gostaria de agradecer a todos os professores e funcionários da Unidade Acadêmica de Matemática da UFCG. Em especial, aos professores: Antônio Pereira Brandão Júnior, por ter me orientado neste trabalho e ter me ensinado tantas coisas, não apenas acerca da matemática como também da vida; Daniel Cordeiro de Morais Filho, pelos anos de tutoria no Grupo PET-Matemática UFCG, tutoria essa, que culminou em diversas lições que me servirão para toda a vida.

Finalmente agradeço aos amigos do curso, especialmente os do Grupo Pet-Matemática UFCG, por estarem presentes em tantos dias e noites em seções de estudos, exercícios, seminários e momentos de descontração. Como também pelo apoio e incentivo dados.

Obrigado!

Resumo

Neste trabalho, empregaremos diversas técnicas decorrentes da Teoria dos Grupos e da Teoria dos Corpos, como também algumas ferramentas analíticas e alguns tópicos introdutórios de álgebra comutativa, para estudarmos os grupos aditivos e multiplicativos de anéis e corpos. Em nossa abordagem, além do estudo de anéis particulares, apresentaremos propriedades interessantes de grupos aditivos e multiplicativos de anéis, bem como condições necessárias e/ou suficientes para que determinado grupo seja grupo aditivo ou grupo multiplicativo de algum corpo ou anel com unidade. Além disso, utilizando estas propriedades e a classificação dos grupos de ordem menor do que ou igual a 11, determinaremos quais desses grupos são grupos multiplicativos de algum anel.

Abstract

In this work we will use multiple techniques deriving of the Theory of Groups and the Theory of Fields, as well as some analytic tools and intrdutory topics of comutative algreba, to study additive and multiplicative groups of rings and fields. In our appoach, even as a study of particular rings, we will present interesting properties of additve and multiplicative groups of rings, as well as necessary and/or sufficient conditions for a group to be and addtive or a multiplicative group of some field or some ring with unity. Furthermore, using these properties and the classification of groups of order 11 or lower, we will determine which os these groups are multiplicative groups of a ring.

Sumário

Introdução

O conceito de grupos foi estabelecido de forma independente pelos matemáticos Walter Von Dyc (1856-1934) e Heinrich Weber (1842-1913), por volta de 1882. Entretanto, fontes históricas indicam que as raízes desse conceito são bem mais antigas, como é possível notar analisando-se os trabalhos de Leonhard Euler (1707-1783) acerca dos restos de uma divisão das potências de um número por um primo pré-fixado (atualmente sabe-se que o conjunto destes restos munido da sua multiplicação usual é um grupo). Também ficam evidentes as raízes do conceito de grupos, nos estudos de Lagrange (1736-1813), Abel (1802-1829) e Galois (1811-1832) sobre permutações de raízes de um polinômio, uma vez que posteriormente comprovou-se que estas permutações de raízes são de fato elementos de um grupo.

O conceito de anéis tem sua raízes históricas no estudo de polinômios em uma ou várias variáveis, e também no estudo de inteiros algébricos. Foi o matemático David Hilbert (1862-1943) o primeiro a utilizar a terminologia *anel* para se referir a estas estruturas.

Motivados inicialmente por ideias clássicas como polinômios e suas raízes, os conceitos de grupos e anéis tornaram-se com o tempo objetos de estudos independentes constituindo duas grandes e importantes áreas dentro da álgebra abstrata: a Teoria dos Grupos e a Teoria dos Anéis.

Atualmente a ligação entre os estudos de grupos e anéis é bastante conhecida, uma vez que ao nos depararmos com o conceito de anéis um fato que se pode observar é que ao descartamos a operação de multiplicação e considerarmos apenas o conjunto munido de sua operação de adição obtemos um grupo abeliano. Observa-se também que o mesmo fato ocorre caso o anel em questão seja um anel com unidade e consideramos apenas o conjunto dos elementos inversíveis do anel munido da operação de multiplicação. Assim, surgem naturalmente a questão do "processo inverso", que servirá como principal motivação deste trabalho. Mais precisamente,

• Dado um grupo abeliano G, é possível definir uma operação de multiplicação que o torne um anel?

• Dado um grupo G, existe algum anel com unidade cujo grupo multiplicativo seja isomorfo a G?

A primeira questão em sua generalidade tem resposta positiva, conforme veremos no texto. Entretanto, podemos particularizar essa questão, bastando exigirmos um pouco mais do anel, como, por exemplo, que tenha unidade ou que seja um domínio de integridade. Observemos que essas particularizações tornam a questão mais enriquecedora, embora mais delicada e difícil de se responder.

Quanto à segunda questão, observa-se que em sua generalidade não é uma questão de fácil resposta.

Além de proporcionar uma melhor compreensão da estrutura de grupos aditivos e multiplicativos de corpos e anéis, uma justificativa para se empreender esse estudo é a de se familiarizar com diversas técnicas e observar, dentro desse contexto, a conexão entre as sub-áreas citadas anteriormente, além de motivar um estudo posterior em tópicos mais avançados da Teoria de Grupos e da Teoria de Anéis.

Este trabalho tem como objetivos estudar a estrutura de grupos aditivos e multiplicativos de anéis e corpos, determinar condições necessárias e/ou suficientes para que um grupo seja grupo aditivo ou grupo multiplicativo de algum corpo ou anel (e com isso tentar responder, ao menos parcialmente, as questões motivadoras) e realizar uma descrição dos grupos aditivo e multiplicativo de alguns corpos anéis clássicos.

Para atingirmos o objetivo deste projeto, faremos uso de uma grande variedade de técnicas que abordam tópicos de diversas sub-áreas da matemática como: Teoria dos Grupos, Teoria do Anéis e Teoria dos Corpos, como também algumas ferramentas analíticas e alguns tópicos introdutórios de álgebra comutativa. Entretanto, inicialmente estudaremos alguns conceitos preliminares, necessários para o entendimento destas técnicas.

No capítulo 2, estudaremos a estrutura de alguns anéis clássicos, tais como o anel $\mathbb{Z}_n$, o anel dos endomorfismos de um grupo abeliano, o anel dos quatérnios e o anel $\mathbb{Z}[\sqrt{p}]$, e faremos uso das técnicas mencionadas anteriormente para determinarmos propriedades intrínsecas a grupos aditivos e multiplicativos de anéis, e a partir destas propriedades buscaremos encontrar condições necessárias e/ou suficientes para que determinado grupo seja grupo aditivo ou grupo multiplicativo de algum anel. Neste mesmo capítulo, faremos também um estudo dos grupos de ordem menor do que ou igual a 11 com o intuito de determinarmos quais deles são grupos multiplicativos de algum anel.

No capítulo 3, faremos um estudo de grupos aditivos e grupos multiplicativos no caso particular em que o anel é um corpo, focando nas ideias de conjuntos geradores e torção, bem como na relação entre os grupos aditivo e multiplicativo de um mesmo corpo.

Capítulo 1

Resultados Preliminares

Neste capítulo apresentaremos os conceitos básicos e resultados inciais que servirão como base para o desenvolvimento deste trabalho.

Dividiremos este capítulo em 3 seções: a primeira irá tratar do conceito de grupos e de suas propriedades básicas, a segunda tratará de anéis e de propriedades referentes a este conceito, e a última seção será dedicada a estabelecer o conceito de corpos e a apresentar os resultados sobre corpos que serão necessários ao longo deste trabalho.

Entretanto, destacamos que no decorrer deste trabalho iremos assumir que o leitor conheça os conceitos e resultados básicos da álgebra linear, assim como os conceitos e resultados básicos referentes a aritmética. Para um leitor interessado em um estudo mais detalhado desses conceitos e resultados indicamos as referências [8] e [7], referentes a álgebra linear e aritmética, respectivamente.

1.1 Grupos

1.1.1 Grupos e Subgrupos

Nesta seção iremos recordar os conceitos de grupos e subgrupos além de destacar os resultados acerca destas estruturas que serão utilizados ao longo deste trabalho. Entretanto, indicamos as referências [5], [6], [10] e [12] para um leitor que deseje um estudo mais detalhado e minucioso destas estruturas e suas propriedades, assim como para as demonstrações dos resultados apresentados nesta seção.

Definição 1. Sejam G um conjunto não vazio e $* \ : G \times G \longrightarrow G$ uma operação em G. Dizemos que $(G, *)$ é um grupo se as seguintes condições são satisfeitas:

i) " $*$ " é associativa, ou seja, $(a * b) * c = a * (b * c)$, para quaisquer $a, b, c \in G$;

ii) Existe $e \in G$ tal que $a * e = e * a = a$ para todo $a \in G$. Um elemento e nessas condições é chamado um elemento neutro de G.

iii) Para cada $a \in G$, existe $a^{-1} \in G$ tal que $a * a^{-1} = a^{-1} * a = e$. Um elemento a^{-1} nessas condições é dito um simétrico, ou inverso, para a em G.

Em geral, denotaremos um grupo $(G, *)$ simplesmente por G, ficando a operação subentendida, e $a * b$ por ab.

Definição 2. Dizemos que um grupo G é abeliano se $ab = ba$ para quaisquer $a, b \in G$.

Destaquemos agora algumas observações importantes a respeito do conceito de grupo.

Observação 1. *Seja G um grupo. Então, valem:*

i) *G possui um único elemento neutro;*

ii) *Para cada $a \in G$ existe um único inverso para a em G. Ademais, $(a^{-1})^{-1} = a$ para qualquer $a \in G$;*

iii) *Se $a, b \in G$, então $(ab)^{-1} = b^{-1}a^{-1}$. Mais geralmente falando, se $a_1, a_2, ..., a_n \in G$, então $(a_1a_2...a_n)^{-1} = {a_n}^{-1}... \ {a_2}^{-1}{a_1}^{-1}$;*

iv) ***Leis do Cancelamento:*** *Se $a, x, y \in G$, então*

$$ax = ay \implies x = y \quad e \quad xa = ya \implies x = y.$$

Estabeleçamos agora dois tipos de notações para grupos que serão utilizadas no decorrer deste trabalho.

1) **Notação Aditiva:** Neste tipo de notação temos:

- Operação: "+".
- Elemento Neutro: "0".
- Inverso de $a \in G$: "$-a$".

2) **Notação Multiplicativa:** Neste tipo de notação temos:

- Operação: "$\cdot$" ou "$*$".
- Elemento Neutro: "e" ou "1".
- Inverso de $a \in G$: "a^{-1}".

Fixemos agora também que neste capítulo o símbolo e sempre irá denotar o elemento neutro de um grupo G, salvo quando dito o contrário.

Um outro conceito que será largamente utilizado ao longo deste trabalho é a ideia de potências de elementos de um grupo, conceito este que iremos estabelecer agora.

Definição 3. Sendo G um grupo, $a \in G$ e $n \in \mathbb{Z}$, definimos

$$a^n = \begin{cases} e & , \text{se } n = 0. \\ \underbrace{aa...a}_{n \ vezes} & , \text{se } n > 0. \\ \\ (a^{-1})^{|n|} & , \text{se } n < 0. \end{cases}$$

E em notação aditiva:

$$na = \begin{cases} e & , \text{se } n = 0. \\ \underbrace{a + a + ... + a}_{n \ parcelas} & , \text{se } n > 0. \\ \\ |n|(-a) & , \text{se } n < 0. \end{cases}$$

Observemos agora algumas propriedades que decorrem da definição anterior.

Observação 2. *Seja G um grupo. Para $a \in G$ e $m, n \in \mathbb{Z}$ valem:*
i) $(a^{-1})^n = (a^n)^{-1} = a^{-n}$;
ii) $a^{n+m} = a^m a^n$;
iii) $(a^m)^n = a^{mn}$.

Definição 4. Sendo G um grupo e A e B subconjuntos não vazios de G definimos:
i) $AB = \{ab \ / \ a \in A \text{ e } b \in B\}$.
ii) $A^{-1} = \{a^{-1} \ / \ a \in A\}$.
Ou em notação aditiva:
i) $A + B = \{a + b \ / \ a \in A \text{ e } b \in B\}$.
ii) $-A = \{-a \ / \ a \in A\}$.

Estabeleçamos também o conceito de ordem de um grupo, assim como o conceito de ordem de um elemento num grupo.

Definição 5. Seja G um grupo. Se G é finito, definimos a ordem de G, denotada por $|G|$, como sendo o número de elementos de G. Caso contrário, dizemos que G é infinito ou que G tem ordem infinita.

Definição 6. Sejam G um grupo e $a \in G$. Dizemos que:
i) a tem ordem infinita (em símbolos, $o(a) = \infty$) se não existe $n \in \mathbb{N}$ tal que $a^n = e$;
ii) a tem ordem finita se existe $n \in \mathbb{N}$ tal que $a^n = e$. Neste caso, definimos a ordem de a, denotada por $o(a)$, como sendo

$$o(a) = min\{n \in \mathbb{N} \ / \ a^n = e\}.$$

De posse do conceito de ordem de um elemento de um grupo, podemos estabelecer os conceitos de grupos de torção e de expoente de um grupo.

Definição 7. Sejam G um grupo e $a \in G$. Dizemos que:

i) a é um elemento de torção de G se $o(a)$ é finita;

ii) G é um grupo de torção quando todo elemento de G tem ordem finita;

iii) G é um grupo livre de torção se todo elemento $x \in G - \{e\}$ tem ordem infinita.

Definição 8. Dizemos que um grupo G tem expoente finito quando existe $k \in \mathbb{N}$ tal que $g^k = e$, para todo $g \in G$. Neste caso, definimos o expoente de G, denotado por $exp\ G$, como sendo

$$exp\ G = min\{k \in \mathbb{N}\ /\ g^k = e, \forall\ g \in G\}.$$

Observemos que se G é um grupo de expoente finito, então G é um grupo de torção. Entretanto, ao tratarmos de grupos quociente mais adiante apresentaremos um exemplo que mostrará que a recíproca não é válida, ou seja, que existem grupos de torção cujo expoente não é finito.

Destaquemos agora algumas observações importantes a respeito de ordem de elementos.

Observação 3. *Sejam G um grupo e $a \in G$. Valem:*

i) $o(e) = 1$. *Ademais, se* $o(a) = 1$, *então:* $a = e$;

ii) *Se* $m, n \in \mathbb{Z}$ *e* $o(a) = \infty$, *então* $a^m = a^n \implies m = n$;

iii) *Sendo* $o(a)$ *finita, vale:* $n \in \mathbb{Z}$ *é tal que* $a^n = e$ *se, e somente se,* $o(a)$ *divide* n;

iv) *Se* $m, n \in \mathbb{Z}$ *e* $o(a)$ *é finita, temos*

$$a^m = a^n \Leftrightarrow a^{m-n} = e \Leftrightarrow n \equiv m(mod\ o(a));$$

v) *Se* $o(a) = \infty$, *então* $\{a^n\ /\ n \in \mathbb{Z}\}$ *é infinito. Consequentemente,* G *finito implica que* G *é um grupo de torção;*

vi) *Se* $o(a) = n$ *finita, então* $\{a^n\ /\ n \in \mathbb{Z}\} = \{e, a, ..., a^{n-1}\}$.

Exemplo 1. *Os conjuntos numéricos* $\mathbb{Z}, \mathbb{Q}$ *e* $\mathbb{R}$, *munidos de sua adição usual, são grupos abelianos. Os conjuntos* $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ *e* $\mathbb{R}^* = \mathbb{R} - \{0\}$, *munidos de sua multiplicação usual, são grupos abelianos.*

Exemplo 2. *Sejam* G_1,G_2,...,G_n *grupos e consideremos o produto cartesiano* $G = G_1 \times ... \times G_n$. *Para* $(x_1, ..., x_n), (y_1, ..., y_n)$ *definamos:*

$$(x_1, ..., x_n) * (y_1, ..., y_n) = (x_1 y_1, ..., x_n y_n).$$

Munido dessa operação, G é um grupo, chamado de produto direto de G_1,...,G_n. Observemos que o elemento neutro de G é dado por $(e_1, e_2, ..., e_n)$, onde e_i é o elemento neutro de G_i. Além disso, $G_1, ..., G_n$ são abelianos se, e somente se, G é abeliano. Ademais, observemos que G_1,G_2,...,G_n são finitos se, e somente se, G é finito e vale: $|G| = |G_1|...|G_n|$.

Exemplo 3. *Seja X um conjunto não vazio. Definamos*

$$S_X = \{f : X \longrightarrow X \ / \ f \text{ é bijetora}\}.$$

Temos que S_X, munido da composição de funções ($\circ$) é um grupo, chamado de grupos das permutações de X. Ademais, se X é finito, então S_X é finito e $|S_X| = |X|!$.

Sendo $n \in \mathbb{N}$ e $I_n = \{1, 2, ..., n\}$, denota-se S_{I_n} simplesmente por S_n e vale $|S_n| = n!$.

Exemplo 4. *Consideremos o conjunto*

$$Q_8 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\},$$

onde $i \in \mathbb{C}$. Temos que Q_8, munido da operação produto de matrizes, é um grupo. Ademais, Q_8 é um grupo que possui apenas um elemento de ordem 2, a saber $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

Passemos agora ao estudo de subgrupos de um grupo.

Definição 9. Seja G um grupo. Definimos um subgrupo de G como sendo um subconjunto H não vazio de G tal que:
i) $xy \in H$, para quaisquer $x, y \in H$;
ii) $x^{-1} \in H$, para todo $x \in H$.

Ou Equivalentemente:
i) $xy^{-1} \in H$, para todos $x, y \in H$.

Adotaremos a notação $H \leq G$ para denotar que H é um subgrupo do grupo G. Observemos que se $H \leq G$, então $e \in H$ e H é por si um grupo. Ademais, observemos que os subgrupos de H são exatamente os subgrupos de G contidos em H.

Exemplo 5. *Sendo G um grupo, $\{e\}$ e G são subgrupos de G, chamados subgrupos triviais.*

Exemplo 6. *Seja H um subconjunto finito não vazio de um grupo G. Se $xy \in H$ para quaisquer $x, y \in H$, então $H \leq G$.*

Exemplo 7. *Se G é um grupo abeliano e $H, K \leq G$, então*

$$HK = \{hk \ / \ h \in H \ e \ k \in K\}$$

é um subgrupo de G.

Exemplo 8. *Sendo $(G, *)$ um grupo e X um conjunto não vazio, consideremos H o conjunto de todas as funções de X em G e definamos*

$$\begin{aligned} + : H \times H &\longrightarrow H \\ (f, g) &\longmapsto f + g \end{aligned}$$

onde $(f + g)(x) = f(x) * g(x)$ para todo $x \in X$. Temos que $(H, +)$ é um grupo. Ademais, G é abeliano se, e somente se, H é abeliano.

Dizemos que uma função $f \in H$ é quase nula quando o conjunto $\{x \in X \ / \ f(x) \neq e\}$ é finito. Observa-se que o subconjunto das funções quase nulas de H é um subgrupo de H

Exemplo 9. *Sendo G um grupo, denotamos por $T(G)$ o conjunto dos elementos de torção de G. Se G é um grupo abeliano, então $T(G) \leq G$.*

Exemplo 10. *Sejam G um grupo e $\emptyset \neq S \subseteq G$. Definimos o centralizador de S em G, denotado por $C_G(S)$, como sendo*

$$C_G(S) = \{g \in G \ / \ gx = xg \ , \forall \ x \in S\}.$$

Observemos que $C_G(S) \leq G$, para qualquer $\emptyset \neq S \subseteq G$. Particularmente, se $a \in G$, definimos $C_G(a) = C_G(\{a\}) = \{g \in G \ / \ ga = ag\}$.

No caso particular em que $S = G$, o centralizador $C_G(G)$ é denotado por $Z(G)$, e é dito o centro de G. Ademais, $Z(G) = G$ se, e somente se, G é abeliano.

Observemos que se G é um grupo e $H \leq G$, particularmente temos $H \subseteq G$. Assim, se G é finito naturalmente temos $|H| \leq |G|$. Ademais, o teorema a seguir nos dá um relação mais específica entre $|H|$ e $|G|$, no caso em que G é um grupo finito.

Teorema 1. ***Teorema de Lagrange.*** *Sejam G um grupo finito e $H \leq G$. Então H é finito e $|H|$ divide $|G|$.*

É importante destacar que a recíproca do Teorema de Lagrange não é válida em geral. Entretanto, no caso particular em que o grupo é abeliano, então vale a recíproca do Teorema de Lagrange e sua demonstração pode ser vista como uma consequência do primeiro Teorema de Sylow, o qual pode ser consultado em [5], páginas 235 e 236.

Diretamente do Teorema de Lagrange decorrem algumas consequências que serão listadas a seguir e que as utilizaremos em diversas ocasiões ao longo deste trabalho.

Corolário 1. *Seja G um grupo finito. Então, valem:*

1) *Se G é um grupo de ordem prima, então $\{e\}$ e G são os únicos subgrupos de G;*

2) *Se $g \in G$, então $o(g)$ divide $|G|$ e consequentemente $g^{|G|} = e$;*

3) *Se $H, K \leq G$, então ambos são finitos e $|H \cap K|$ divide $|H|$ e $|K|$. Particularmente, se $mdc(|H|, |K|) = 1$, então $H \cap K = \{e\}$.*

Um comentário pertinente a respeito de ordem de subgrupos de um grupos G é o fato que se $H, K \leq G$ e H, K são finitos, então o produto HK é finito e vale:

$$|HK| = \frac{|H||K|}{|H \cap K|} \ .$$

Nos dediquemos agora ao estudo de subgrupos gerados por subconjuntos e suas propriedades relevantes neste trabalho.

Definição 10. Sejam G um grupo e S um subconjunto não vazio de G. Definimos o subgrupo de G gerado por S, denotado por $< S >$, como sendo

$$< S >= \{x_1 \cdot x_2 \cdot ... \cdot x_n \ / \ n \in \mathbb{N}, x_i \in S \cup S^{-1}\}.$$

Se $S \subseteq G$ é um conjunto finito, digamos $S = \{x_1, x_2, ..., x_n\}$, então denotamos $< S >$ por $< x_1, x_2, ..., x_n >$. Ademais, se S é unitário, digamos $S = \{a\}$, então denotamos $< S >$ por $< a >$ e vale

$$< S >=< a >= \{a^n \ / \ n \in \mathbb{Z}\}.$$

Observemos que se $o(a) = \infty$, então $< a >$ é infinito. Por outro lado, se $o(a)$ é finita, então $< a >$ é finito e vale $| < a > | = o(a)$ (veja a Observação 3, página 16).

Exemplo 11. *Dado $n \in \mathbb{N}$, definimos o grupo diedral n, denotado por D_n, como sendo $D_n =< a, b >$, onde $o(a) = n$, $o(b) = 2$ e $bab = a^{n-1}$. Observemos que $|D_n| = 2n$.*

Definição 11. Seja G um grupo. Dizemos que um subconjunto S de G é um conjunto gerador de G (ou que gera G) se $< S >= G$. Ademais, se G possui um conjunto gerador finito dizemos que G é finitamente gerado.

Um fato curioso a respeito de grupos finitamente gerados é o fato que existem grupos finitamente gerados que possuem subgrupos que não são finitamente gerados. Entretanto, tal "patologia" não ocorre em grupos abelianos, conforme mostra o teorema a seguir.

Teorema 2. *Sejam G um grupo abeliano finitamente gerado e $H \leq G$. Então, H é finitamente gerado.*

Definição 12. Um grupo G é dito cíclico quando existe $a \in G$ tal que $G =< a >$.

Observemos que se G é um grupo cíclico, digamos $G =< a >$, então G é abeliano e $|G| = o(a)$. Uma outra observação a respeito de grupos cíclicos é que subgrupos de um grupo cíclico são ainda grupos cíclicos. Ademais, em determinadas condições o produto de subgrupos cíclicos é ainda um grupo cíclico, conforme mostra o teorema a seguir.

Teorema 3. *Sejam G um grupo abeliano e $A, B \leq G$ tais que A e B são cíclicos e de ordens finitas. Se $mdc(|A|, |B|) = 1$, então AB é um grupo cíclico.*

1.1.2 Subgrupos Normais e Grupos Quocientes

Nesta seção iremos definir subgrupos normais e grupos quociente, além de destacar as propriedades destas estruturas que serão revelantes ao longo deste trabalho. Para um leitor interessado nas demonstrações dos resultados apresentados nesta seção e num estudo mais detalhado destas estruturas indicamos as referências [5], [6], [10] e [12].

Definição 13. Sejam G um grupo, H um subgrupo de G e $g \in G$. Definimos a classe lateral à direita de H contendo g, denotada por Hg, como sendo $Hg = \{hg \ / \ h \in H\}$. Definimos também a classe lateral à esquerda de H contendo g, denotada por gH, como sendo $gH = \{gh \ / \ h \in H\}$.

Definição 14. Sejam G um grupo e $H \leq G$. Dizemos que H é um subgrupo normal de G, e denotamos por $H \trianglelefteq G$, se $gH = Hg$ para todo $g \in G$.

Observemos que sendo G um grupo, sempre temos $\{e\} \trianglelefteq G$ e $G \trianglelefteq G$. Ademais, diremos que um grupo G é um grupo *simples* quando $\{e\}$ e G são os únicos subgrupos normais de G.

Exemplo 12. *Se G é um grupo abeliano, então todo subgrupo de G é normal em G.*

Destaquemos agora a seguinte propriedade de subgrupos normais.

Observação 4. *Sejam G um grupo e $H, K \leq G$. Então, se $H \trianglelefteq G$ ou $K \trianglelefteq G$, temos $HK \leq G$. Ademais, se $H \trianglelefteq G$ e $K \trianglelefteq G$, temos $HK \trianglelefteq G$.*

Passemos agora ao estudo do conceito de grupos quocientes. Sejam G um grupo, $N \trianglelefteq G$ e $\frac{G}{N} = \{gN \ / \ g \in G\}$. Observemos que $aN = bN$ se, e somente se, $a^{-1}b \in N$. Particularmente, $aN = N$ se, e somente se, $a \in N$.

Definamos em $\frac{G}{N}$ a seguinte operação

$$\begin{aligned} \cdot : \frac{G}{N} \times \frac{G}{N} &\longrightarrow \frac{G}{N} \\ (aN, bN) &\longmapsto (aN) \cdot (bN) = (ab)N \ . \end{aligned}$$

A operação " $\cdot$ " está bem definida e temos que $\frac{G}{N}$, munido desta operação, é um grupo, chamado de grupo quociente de G por N. Observemos que $eN = N$ é o elemento neutro de $\frac{G}{N}$ e que se $g \in G$, então $(gN)^{-1} = g^{-1}N$ em $\frac{G}{N}$.

Quando não houver perigo de confusão em relação a que grupo quociente estamos tratando, iremos denotar gN simplesmente por $\overline{g}$, ficando subentendido que o quociente é em relação ao subgrupo N.

Exemplo 13. *Consideremos $\mathbb{Q}$ e $\mathbb{Z}$ os grupos aditivos dos racionais e dos inteiros, respectivamente. Notemos que $\mathbb{Z} \trianglelefteq \mathbb{Q}$, uma vez que $\mathbb{Q}$ é abeliano. Ademais, observemos que dado $\overline{x} \in \frac{\mathbb{Q}}{\mathbb{Z}}$, temos que $\overline{x} = \overline{m/n}$, com $n, m \in \mathbb{Z}$ e $n > 0$. Assim,*

$$n\overline{x} = n\overline{m/n} = \overline{mn/n} = \overline{m} = \overline{0} \ .$$

Logo, $\overline{x}$ é um elemento de torção de $\frac{\mathbb{Q}}{\mathbb{Z}}$ e da arbitrariedade de $\overline{x}$ segue que $\frac{\mathbb{Q}}{\mathbb{Z}}$ é um grupo de torção. Entretanto, uma vez que não há limite para a ordem dos elementos de $\frac{\mathbb{Q}}{\mathbb{Z}}$, pois para cada $n \in \mathbb{N}$ temos $o(\overline{1/n}) = n$, segue que $exp \ \frac{\mathbb{Q}}{\mathbb{Z}}$ não é finito. Fica assim comprovado que existem grupos de torção cujo expoente não é finito.

Para finalizar esta seção, iremos destacar agora algumas propriedades referentes a grupos quocientes.

Observação 5. *Sendo G um grupo e $N \trianglelefteq G$, temos:*

1) *Se G é finito, então $\frac{G}{N}$ é finito e $|\frac{G}{N}| = \frac{|G|}{|N|}$;*
2) *Se G é abeliano, então $\frac{G}{N}$ é abeliano;*
3) *Se $g \in G$ e $n \in \mathbb{Z}$, então $\overline{g}^n = \overline{g^n}$. Consequentemente, se G é cíclico, então $\frac{G}{N}$ é cíclico. Mais precisamente, se $G =< a >$, então $\frac{G}{N} =< \overline{a} >$.*

1.1.3 Homomorfismos de Grupos

Nesta seção iremos definir o conceito de homomorfismos de grupos além de destacar as propriedades e resultados provenientes deste conceito que serão revelantes ao longo deste trabalho. Entretanto, para um leitor interessado nas demonstrações e num estudo mais detalhado das ideias e resultados que apresentaremos nesta seção indicamos as referências [5], [6], [10] e [12].

Definição 15. Sejam G e G_1 grupos. Uma aplicação $f : G \longrightarrow G_1$ é dita um homomorfismo de grupos se satisfaz

$$f(xy) = f(x)f(y),$$

para quaisquer $x, y \in G$.

Sendo $f : G \longrightarrow G_1$ um homomorfismo de grupos, definimos:
• O núcleo de f, denotado por $Ker\ f$, como sendo

$$Ker\ f = \{x \in G\ /\ f(x) = e_1\},$$

onde e_1 é o elemento neutro de G_1.
• A imagem de f, denotada por Imf, como sendo

$$Imf = \{f(x)\ /\ x \in G\}.$$

Algumas importantes propriedades de homomorfismos de grupos que gostaríamos de destacar são as propriedades a seguir.

Observação 6. *Sejam G e G_1 grupos e $f : G \longrightarrow G_1$ um homomorfismo. Valem:*

a) $f(e) = e_1$ (e_1 é o elemento neutro de G_1);

b) $f(x^{-1}) = f(x)^{-1}$, para todo $x \in G$;

c) $f(x^n) = f(x)^n$, para quaisquer $x \in G$ e $n \in \mathbb{Z}$;

d) Se $H \leq G$, então $f(H) = \{f(h)\ /\ h \in H\}$ é subgrupo de G_1. Particularmente, Imf é um subgrupo de G_1;

e) Se $K \leq G_1$, então $f^{-1}(K) = \{x \in G\ /\ f(x) \in K\}$ é um subgrupo de G. Ademais, se $K \trianglelefteq G_1$, então $f^{-1}(K) \trianglelefteq G$. Particularmente, ker $f \trianglelefteq G$;

f) f é injetiva se, e somente se, $Ker\ f = \{e\}$.

Definição 16. Definimos isomorfismo de grupos como sendo um homomorfismo bijetivo de grupos.

Se G e G_1 são grupos e existe um isomorfismo $f : G \longrightarrow G_1$, dizemos que G é isomorfo a G_1, e denotamos $G \simeq G_1$. Neste caso, temos que $f^{-1} : G_1 \longrightarrow G$ é também um isomorfismo.

Exemplo 14. *Sejam G um grupo abeliano e $n \in \mathbb{N}$. Então a aplicação*

$$\begin{aligned} f : G &\longrightarrow G \\ x &\longmapsto f(x) = x^n \end{aligned}$$

é um homomorfismo de grupos. Ademais, se G é finito e $mdc(n, |G|) = 1$, então f é um isomorfismo.

Exemplo 15. *Sejam G_1, G_2 e G_3 grupos, $f : G_1 \longrightarrow G_2$ e $g : G_2 \longrightarrow G_3$ homomorfismos de grupos. Temos que a aplicação $g \circ f : G_1 \longrightarrow G_3$ é também um homomorfismo de grupos.*

Exemplo 16. *Sejam G e H grupos cíclicos. Se $|G| = |H|$, então $G \simeq H$.*

Exemplo 17. *Seja G um grupo. Se $\varphi : G \longrightarrow G$ é um isomorfismo, dizemos que φ é um automorfismo de G. Observemos que a função identidade de G é um automorfismo de G. Ademais, denotando por $Aut\ G$ o conjunto de todos os automorfismos de G, temos que $AutG$ munido da composição de funções é um grupo, chamado de grupo dos automorfismos de G.*

Uma propriedade bastante útil proveniente do conceito de isomorfismos de grupos é dada pela proposição a seguir.

Proposição 1. *Sejam G, G_1 grupos e $f : G \longrightarrow G_1$ um isomorfismo. Se $x \in G$ é tal que $o(x) = n$, então $o(f(x)) = n$ em G_1.*

Além de preservar ordem, como mostra a Proposição 1, isomorfismos de grupos também preservam conjuntos geradores conforme mostra a proposição a seguir.

Proposição 2. *Sejam G, G_1 grupos e $f : G \longrightarrow G_1$ um isomorfismo. Se $X \subset G$ é tal que $< X >= G$, então $< f(X) >= G_1$.*

Enunciaremos agora o Teorema Fundamental dos Homomorfismos, este resultado será deveras necessário para a demonstração de diversos resultados que apresentaremos neste trabalho. Enunciaremos também uma consequência deste teorema, o Segundo Teorema do Isomorfismo, que se fará presente em várias ocasiões ao longo deste trabalho.

Teorema 4. ***Teorema Fundamental dos Homomorfismos:*** *Sejam G, G_1 grupos, $f : G \longrightarrow G_1$ um homomorfismo e $N = Ker\ f$. Então a aplicação*

$$\begin{aligned} \overline{f} : \frac{G}{N} &\longrightarrow Im\ f \\ \overline{g} &\longmapsto \overline{f}(\overline{g}) = f(g) \end{aligned}$$

é bem definida e é um isomorfismo, e assim $\frac{G}{N} \simeq Im\ f$.

Teorema 5. ***Segundo Teorema do Isomorfismo:*** *Sejam G um grupo e $H, N \leq G$, com $N \trianglelefteq G$. Então, $H \cap N \trianglelefteq H$ e $\frac{H}{H \cap N} \simeq \frac{HN}{N}$.*

Para finalizar esta seção, apresentaremos agora a classificação dos grupos de ordem menor ou igual a 11, a menos de isomorfismos.

A classificação dos grupos de ordem menor ou igual a 11, a menos de isomorfismos, está explicitada na tabela a seguir e a demonstração desta classificação pode ser encontrada em [5], nas páginas 169-176. Na Tabela 1.1 C_n irá denotar um grupo cíclico de ordem n. Recordemos que C_n é o único grupo cíclico de ordem n, a menos de isomorfismos, conforme comentamos no Exemplo 16.

n	Grupos de ordem n
1	C_1
2	C_2
3	C_3
4	C_4 e $C_2 \times C_2$
5	C_5
6	C_6 e S_3
7	C_7
8	C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_4 e Q_8
9	C_9 e $C_3 \times C_3$
10	C_{10} e D_5
11	C_{11}

Tabela 1.1: Grupos de Ordem menor ou igual a 11, a menos de isomorfismo.

1.2 Anéis

1.2.1 Anéis e Subanéis

Nesta seção iremos relembrar os conceitos de anéis e subanéis. Além disso, destacaremos os resultados acerca destes conceitos que serão utilizados ao longo deste trabalho. Indicamos as referências [4], [6], [10] e [12] para um estudo mais detalhado destes conceitos, como também para as demonstrações dos resultados elencados nesta seção.

Inicialmente recordemos a definição de anéis.

Definição 17. Sejam A um conjunto não vazio e "+", "$\cdot$"duas operações em A. Dizemos que a terna $(A, +, \cdot)$ é um anel quando valem:

i) $(A, +)$ é um grupo abeliano;

ii) $(ab)c = a(bc)$, para quaisquer $a, b, c \in A$;

iii) $a(b + c) = ab + ac$ e $(a + b)c = ac + bc$, para quaisquer $a, b, c \in A$.

Sendo $(A, +, \cdot)$ um anel, as operações "+"e "$\cdot$" são chamadas de adição e multiplicação do anel $(A, +, \cdot)$. Ademais, quando não houver perigo de confundir estas operações, iremos denotar o anel $(A, +, \cdot)$ simplesmente por A.

Definição 18. Seja A um anel. Se A é finito, definimos a ordem de A, denotada por $|A|$, como sendo a quantidade de elementos de A. Caso contrário, diremos que a ordem de A é infinita.

Podemos definir também alguns casos especiais de anéis exigindo um pouco mais da operação de multiplicação.

Definição 19. Seja A um anel. Dizemos que:

i) A é um anel comutativo se a multiplicação é comutativa, isto é, $ab = ba$ para quaisquer $a, b \in A$;

ii) A é um anel com unidade se existe $1_A \in A$ tal que $a1_A = 1_A a = a$, para todo $a \in A$. O elemento 1_A (único nessas condições) é chamado de unidade do anel A.

Destaquemos agora algumas observações acerca do conceito de anéis.

Observação 7. *Sendo A um anel, temos:*

i) Existe um único elemento $0 \in A$ (também denotado por 0_A) tal que 0 é o elemento neutro da adição, isto é, $0 + a = a$, para todo $a \in A$. Este elemento é dito o zero do anel A;

ii) Dado $a \in A$, existe um único elemento $-a \in A$, tal que $a + (-a) = 0$. O elemento $-a$ é chamado de oposto aditivo de a em A. Ademais, é fácil ver que $-(-a) = a$.

iii) Se $a, b, c \in A$ são tais que $a+b = a+c$, então $b = c$ (vide Observação 1, página 14);

iv) Podemos definir uma operação de subtração em A da seguinte forma:

$$\begin{aligned} - : \ & A \times A \longrightarrow A \\ & (a,b) \longmapsto \ a - b = a + (-b) \ . \end{aligned}$$

Analogamente ao feito para grupos, sendo A um anel e $n \in \mathbb{Z}$, podemos definir na e a^n, para $a \in A$.

Definição 20. Sendo A um anel, $a \in A$ e $n \in \mathbb{Z}$, definimos

$$na = \begin{cases} 0_A & , \text{se } n = 0. \\ \underbrace{a + a + ... + a}_{n \ parcelas} & , \text{se } n > 0. \\ \\ |n|(-a) & , \text{se } n < 0. \end{cases}$$

Ademais, se $n \geq 0$ definimos

$$a^n = \begin{cases} \underbrace{aa...a}_{n \ vezes} & , \text{se } n > 0 \\ 1_A & , \text{se } n = 0 \text{ e } A \text{ possui unidade.} \end{cases}$$

Destaquemos também algumas propriedades básicas de anéis.

Observação 8. *Sendo A um anel, valem:*

i) $0a = a0 = 0$, para todo $a \in A$;

ii) $(-a)b = a(-b) = -(ab)$, para quaisquer $a, b \in A$;

iii) $(-a)(-b) = ab$, para quaisquer $a, b \in A$;

iv) $a(b-c) = ab - ac$ e $(a-b)c = ac - bc$, para quaisquer $a, b, c \in A$;

v) $(-1)a = a(-1) = -a$, para todo $a \in A$ (se A possui unidade);

vi) Se A é um anel com unidade tal que $1_A = 0$, então $A = \{0\}$. Neste caso, A é dito um anel trivial.

Recordemos agora o conceito de elementos inversíveis de um anel com unidade.

Definição 21. Sejam A um anel com unidade. Dizemos que $a \in A$ é um elemento inversível em A se existe $a^{-1} \in A$, tal que $aa^{-1} = 1_A = a^{-1}a$. Neste caso, o elemento a^{-1} (único nestas condições) e é dito o inverso de a em A.

Sendo A um anel com unidade, iremos denotar o conjunto dos elementos inversíveis de A por $U(A)$. Ademais, prova-se que $(U(A), \cdot)$ é um grupo, o qual iremos tratar em maiores detalhes no Capítulo 2.

Se A é um anel com unidade e $a \in U(A)$, dado $n \in \mathbb{Z}$ com $n < 0$, definimos $a^n := (a^{-1})^{|n|}$.

Tendo recordado o conceito de elementos inversíveis, passemos agora ao conceito de anéis com divisão e corpos.

Definição 22. Seja A um anel com unidade (não trivial). Diremos que:

i) A é um anel com divisão se $U(A) = A - \{0\}$;

ii) A é um corpo se A é um anel com divisão comutativo;

iii) A é um domínio de integridade, ou $D.I.$ se A é comutativo e para $a, b \in A$ vale a implicação:

$$ab = 0 \Longrightarrow a = 0 \text{ ou } b = 0 \ .$$

Iremos apresentar alguns exemplos de anéis que serão importantes ao longo deste trabalho.

Exemplo 18. *Os conjuntos numéricos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$, munidos de sua adição e multiplicação usuais, são anéis comutativos com unidade. Observemos que $U(\mathbb{Z}) = \{-1, 1\}$ e que $\mathbb{Q}, \mathbb{R}$, e $\mathbb{C}$ são corpos.*

Exemplo 19. *Sejam V um espaço vetorial e $\mathcal{L}(V)$ o conjunto de todos os operadores lineares de V. Munido de sua adição usual (soma ponto a ponto) e da composição, $\mathcal{L}(V)$ é um anel com unidade (operador identidade de V). Ademais, temos que $U(\mathcal{L}(V))$ é o conjunto dos operadores lineares de V bijetores, o qual denotaremos por $GL(V)$.*

Exemplo 20. *Seja R um anel e consideremos $M_n(R)$ o conjuntos de todas as matrizes de ordem n com entradas em R. Temos que $M_n(R)$, munido da adição e multiplicação usual de matrizes, é um anel. Além disso, se R é um anel com unidade, então $M_n(R)$ é um anel com unidade. Ademais, sendo R comutativo com unidade, tem-se*

$$U(M_n(R)) = \{A \in M_n(R) \ / \ det(A) \in U(R)\},$$

onde $det(A)$ é definido de maneira análoga à definição de determinante de matrizes com entradas reais.

Exemplo 21. *Sejam R_1,R_2,...,R_n anéis e consideremos o produto cartesiano $R = R_1 \times ... \times R_n$. Para $(x_1, ..., x_n), (y_1, ..., y_n)$ definamos*

$$(x_1, ..., x_n) + (y_1, ..., y_n) = (x_1 + y_1, ..., x_n + y_n)$$

e

$$(x_1, ..., x_n) * (y_1, ..., y_n) = (x_1y_1, ..., x_ny_n) \ .$$

Com essas operações, R é um anel, chamado de produto direto de R_1,...,R_n. Além disso $R_1, ..., R_n$ são comutativos se, e somente se, R é comutativo. Temos também que se $R_1, ..., R_n$ têm unidade, então R tem unidade e valem:

i) $1_R = (1_{R_1}, ..., 1_{R_n})$*, onde* 1_{R_i} *denota a unidade do anel* R_i *;*

ii) $U(R) = U(R_1) \times ... \times U(R_n)$ *.*

Exemplo 22. *Sendo A um anel, definimos um polinômio com coeficientes em A na indeterminada x, como sendo uma expressão da forma*

$$f(x) = \sum_{k=0}^{\infty} a_k x^k = a_0 + a_1x + ... + a_kx^k + ...$$

com $a_i \in A$, para a qual existe $n \in \mathbb{N}$ tal que $a_k = 0$ para $k > n$. Assim, denotamos $f(x) = a_0 + ... + a_nx^n$.

Definimos o grau de um polinômio não nulo $f(x) = a_0 + a_1x + ... + a_nx^n$, denotado por $\partial f(x)$, como sendo

$$\partial f(x) = max\{i \ / \ a_i \neq 0\}.$$

Dizemos que um polinômio é constante se tem grau 0.

Iremos denotar por $A[x]$ o conjunto de todos os polinômios com coeficientes em A na indeterminada x.

Considerando agora $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i \in A[x]$, *definamos*

$$f(x) + g(x) = \sum_{i=0}^{q} c_i x^i, \text{ onde } c_i = a_i + b_i \text{ e } q = max\{n, m\}$$

e

$$f(x)g(x) = \sum_{i=0}^{n+m} d_i x^i, \text{ onde } d_i = \sum_{j=0}^{i} a_i b_{k-i} \ .$$

Temos que $A[x]$ munido das operações definidas acima, é um anel.

Recordemos agora o conceito de subanel e observemos alguns exemplos de subanéis serão relevantes nesse trabalho.

Definição 23. Sejam A um anel e B um subconjunto não vazio de A. Dizemos que B é um subanel de A se satisfaz:

i) $x + y$,$-x \in B$, para quaisquer x, y em B;

ii) $xy \in B$, para quaisquer $x, y \in B$.

Observemos que se B é um subanel de A, então $0 \in B$ e B é por si um anel. Ademais, observemos que os subanéis de B são exatamente os subanéis de A contidos em B.

Exemplo 23. *Se A é um anel, então $\{0\}$ e A são subanéis de A. Ademais, fixado $a \in A$, o conjunto*

$$C(a) = \{x \in A \ / \ xa = ax\}$$

é também um subanel de A, chamado de centralizador de a em A. Definindo ainda

$$Z(A) = \{a \in A \ / \ ax = xa, \ \forall x \in A\}$$

temos que $Z(A)$ é um subanel de A, chamado de centro de A.

Exemplo 24. *Sendo $p \in \mathbb{Z}$ um número primo, consideremos o o conjunto*

$$\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} \ / \ a, b \in \mathbb{Z}\}.$$

Temos que $\mathbb{Z}[\sqrt{p}]$ é um subanel de $\mathbb{R}$ e que $\mathbb{Z} \subset \mathbb{Z}[\sqrt{p}]$.

Para finalizarmos essa seção, iremos recordar o conceito de característica de um anel.

Definição 24. Seja A um anel. Dizemos que A possui característica positiva se existe $n \in \mathbb{N}$ tal que $na = 0$, para todo $a \in A$. Neste caso, definimos a característica de A, denotada por $char\ A$, como sendo

$$char\ A = min\{n \in \mathbb{N} \ / \ na = 0, \forall a \in A\} \ .$$

Se o conjunto $\{n \in \mathbb{N} \ / \ na = 0, \forall a \in A\}$ é vazio, dizemos que A tem característica 0.

Um comentário pertinente a respeito da característica de um anel é o fato de que se A é um anel com unidade tal que $char\ A \neq 0$, então $char\ A = min\{n \in \mathbb{N} \ / \ n1_A = 0\}$.

1.2.2 Ideais e Anéis Quocientes

Nesta seção iremos definir ideais e anéis quocientes, além de destacar as propriedades destas estruturas que serão revelantes ao longo deste trabalho. Indicamos para um leitor interessado em um estudo mais aprofundado destes conceitos, bem como nas demonstrações dos resultados que apresentaremos no decorrer desta seção, as referências [4], [6], [10] e [12].

Definição 25. Sejam A um anel e I um subgrupo aditivo de A (ou seja, um subgrupo de $(A, +)$). Dizemos que I é um ideal de A se $xa, ax \in A$ para quaisquer $a \in A$ e $x \in I$.

Observemos que sendo A um anel $\{0\}$ e A são sempre ideais de A. Ademais, se A e $\{0\}$ são os únicos ideais de A, dizemos que A é um anel simples.

Um fato interessante sobre anéis simples é o teorema a seguir.

Teorema 6. *Se A é um anel simples, comutativo e com unidade, então A é um corpo.*

Destaquemos agora algumas observações a respeito de ideais de um anel.

Observação 9. *Sejam A um anel e I um ideal de A. Valem:*

i) I é um subanel de A;

ii) Se A é um anel com unidade e $I \cap U(A) \neq \emptyset$, então $I = A$.

Exemplo 25. *Sejam A um anel comutativo e com unidade e $x \in A$. Temos que o conjunto $< x >= xA = \{xa \ / \ a \in A\}$ é um ideal de A, chamado de ideal principal gerado por x. Observa-se que $< x >$ está contido em todo ideal de A que contém o elemento x.*

Exemplo 26. *Consideremos o anel $\mathbb{Z}$ dos inteiros. Para cada $n \in \mathbb{Z}$, definamos*

$$n\mathbb{Z} = \{nx \ / \ x \in \mathbb{Z}\}.$$

Temos que $n\mathbb{Z}$ é um ideal de $\mathbb{Z}$ (ideal principal gerado por n). Ademais, é possível mostrar que todos os ideais de $\mathbb{Z}$ são dessa forma.

Passaremos agora aos conceitos de ideais primos e maximais de um anel.

Definição 26. Sejam A um anel comutativo com unidade e I um ideal de A, com $I \subsetneq A$. Dizemos que:

i) I é um ideal primo de A se para $x, y \in A$ vale:

$$xy \in I \implies x \in I \text{ ou } y \in I \ ;$$

ii) I é um ideal maximal de A se não existe nenhum ideal J de A, com $J \neq A$, tal que $I \subsetneq J$.

Uma observação importante a respeito de ideais primos e ideais maximais é que todo ideal maximal é um ideal primo. Ademais, em situações particulares como no caso de anéis finitos também vale a recíproca, ou seja, todo ideal primo é um ideal maximal.

Outra observação importante a respeito de ideais maximais é a seguinte.

Observação 10. *Seja A um anel comutativo com unidade, então valem:*

1) *Se I é um ideal próprio de A, então I está contido em algum ideal maximal de A.*

2) *Se $x \in A - U(A)$, então $x \in M$, para algum M ideal maximal de A.*

Passemos agora ao estudo dos anéis quocientes e de propriedades dessas estruturas.

Definição 27. Se I é um ideal de um anel A e $a \in A$, definimos a classe lateral de I contendo a, denotada por $a+I$, como sendo $a+I = \{a+x \ / \ x \in I\}$.

Observemos que sendo A um anel e I um ideal de A, temos $a+I = b+I$ se, e somente se, $a - b \in I$. Particularmente, $a + I = I$ se, e somente se, $a \in I$.

Sejam A um anel e I um ideal de A. Consideremos

$$\frac{A}{I} = \{\overline{a} = a + I \ / \ a \in A\}$$

e as operações de adição e multiplicação em $\frac{A}{I}$, definidas, respectivamente, por:

$$\overline{a} + \overline{b} = \overline{a+b} = (a+b) + I \quad \text{e} \quad \overline{a}\overline{b} = \overline{ab} = (ab) + I \ .$$

As operações acima estão bem definidas e temos que $\frac{A}{I}$, munido delas, é um anel, chamado de anel quociente de A por I.

Quando não houver perigo de confusão a respeito de que ideal estamos tratando, iremos denotar $a+I$ simplesmente por $\overline{a}$, ficando subentendido que o quociente é em relação ao ideal I.

Destaquemos agora algumas propriedades básicas dos anéis quocientes.

Observação 11. *Sejam A um anel e I um ideal de A. Valem:*

i) $\overline{0} = 0 + I = I$ é o zero do anel quociente $\frac{A}{I}$. Ademais, $a + I = I$ se, e somente se, $a \in I$;

ii) Se $a \in A$, então $\overline{-a} = -\overline{a}$;

iii) Se A é comutativo, então $\frac{A}{I}$ é comutativo;

iv) Se A possui unidade, então $\frac{A}{I}$ possui unidade, a saber $\overline{1} = 1 + I$;

v) $\frac{A}{I} = \{\overline{0}\}$ se, e somente se, $I = A$.

Exemplo 27. *Seja $n \in \mathbb{N}$. Recordemos que do Exemplo 26, o conjunto $n\mathbb{Z}$ é um ideal do anel dos inteiros $\mathbb{Z}$. Assim sendo, faz sentido considerarmos o anel quociente $\frac{\mathbb{Z}}{n\mathbb{Z}}$. Temos que*

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$$

o qual normalmente denotaremos por $\mathbb{Z}_n$. Observe que $\overline{a} = \overline{b}$ em $\mathbb{Z}_n$ $(a, b \in \mathbb{Z})$ se, e somente se, $a \equiv b (mod\ n)$.

Para finalizarmos está seção iremos apresentar um teorema que nos garante que determinados anéis quocientes são corpos.

Teorema 7. *Sejam A um anel comutativo com unidade e I um ideal maximal de A. Então, $\frac{A}{I}$ é um corpo.*

1.2.3 Homomorfismos de Anéis

Nesta seção iremos definir o conceito de homomorfismos de anéis além de destacar as propriedades e resultados provenientes deste conceito que serão revelantes ao longo deste trabalho. Para as demonstrações dos resultados e um estudo mais acurado das ideias que apresentaremos nesta seção indicamos as referências [4], [6], [10] e [12].

Definição 28. Sejam A e A_1 anéis. Uma aplicação $f : A \longrightarrow A_1$ é dita um homomorfismo de anéis se satisfaz

$$f(x+y) = f(x) + f(y)$$

e

$$f(xy) = f(x)f(y)$$

para quaisquer $x, y \in A$.

Sendo $f : A \longrightarrow A_1$ um homomorfismo de anéis, definimos:
• O núcleo de f, denotado por $Ker\ f$, como sendo

$$Ker\ f = \{x \in A\ /\ f(x) = 0_1\},$$

onde 0_1 é o zero de A_1.
• A imagem de f, denotada por Imf, como sendo

$$Imf = \{f(x)\ /\ x \in A\}.$$

Algumas importantes propriedades de homomorfismos de anéis que gostaríamos de destacar são as propriedades a seguir.

Observação 12. *Sejam A e A_1 anéis e $f : A \longrightarrow A_1$ um homomorfismo. Valem:*

a) $f(0_A) = 0$ (onde 0 é o elemento zero de A_1);

b) $f(na) = nf(a)$, para todo $x \in A$ e $n \in \mathbb{Z}$. Ademais, se $n \geq 0$, então $f(a^n) = f(a)^n$;

c) Se B é subanel de A, então $f(B) = \{f(b)\ /\ b \in B\}$ é subanel de A_1. Particularmente, Imf é um subanel de A_1;

d) Se A possui unidade, então $Im\ f$ possui unidade e $f(1_A)$ é a unidade de $Im\ f$;

e) Se S é um subanel de A_1, então $f^{-1}(S) = \{s \in A\ /\ f(s) \in S\}$ é um subanel de A. Ademais, se S é um ideal de A_1, então $f^{-1}(S)$ é um ideal de A. Particularmente, $Ker\ f$ é um ideal de A;

f) f é injetiva se, e somente se, $Ker\ f = \{0_A\}$.

g) Se B_1 e B_2 são subanéis de A, com $Ker\ f \subseteq B_1 \cap B_2$ e $f(B_1) = f(B_2)$, então $B_1 = B_2$.

Exemplo 28. *Sejam A_1, A_2 e A_3 anéis, $f : A_1 \longrightarrow A_2$ e $g : A_2 \longrightarrow A_3$ homomorfismos de anéis. Temos que a aplicação $g \circ f : A_1 \longrightarrow A_3$ é também um homomorfismo de anéis.*

Definição 29. Definimos isomorfismo de anéis como sendo um homomorfismo bijetivo de anéis.

Se A e A_1 são anéis e existe um isomorfismo $f : A \longrightarrow A_1$, dizemos que A é isomorfo a A_1, e denotamos por $A \simeq A_1$. Neste caso, temos que $f^{-1} : A_1 \longrightarrow A$ é também um isomorfismo.

Para finalizarmos esta seção, enunciaremos o Teorema Fundamental dos Homomorfismos para Anéis (recordemos que um resultado análogo foi apresentado para grupos no Teorema 4). Enunciaremos também, como uma consequência deste teorema, o Segundo Teorema do Isomorfismo para anéis, um resultado análogo ao Teorema 5, que se fará presente em várias ocasiões ao longo deste trabalho.

Teorema 8. ***Teorema Fundamental dos Homomorfismos:*** *Sejam A,A_1 anéis, $f : A \longrightarrow A_1$ um homomorfismo e $I = Ker\ f$. Então, $\frac{A}{I} \simeq Im\ f$.*

Teorema 9. ***Segundo Teorema do Isomorfismo:*** *Sejam A um anel, S um subanel de A, e I um ideal de A. Então, $S \cap I$ é ideal de S e $\frac{S+I}{I} \simeq \frac{S}{S \cap I}$.*

1.2.4 Domínios de Fatoração Única e Corpos de Frações

Nesta seção iremos definir o conceito de domínio de fatoração única (DFU) e de corpo de frações de um DFU. Além disso, ressaltaremos as propriedades e resultados provenientes destes conceitos que utilizaremos ao longo deste trabalho. Indicamos contudo as referências [4] e [12] para um leitor interessado em um estudo mais detalhado dos conceitos e demonstração dos resultados comentados nesta seção.

Entretanto, antes de apresentarmos a definição de um DFU iremos definir elementos irredutíveis e elementos associados em um domínio de integridade.

Definição 30. Sejam D um domínio de integridade e $a, b \in D$. Dizemos que:

i) a divide b em D se existe $c \in D$ tal que $b = ac$;

ii) a é associado a b em D, e denotamos $a \sim b$, se existe $x \in U(D)$ tal que $a = bx$;

iii) d é um máximo divisor comum de a, b em D, e denotamos por $mdc(a, b) = d$, se d divide a e b e sempre que c dividir a e b tivermos que c divide d;

iv) a e b são relativamente primos em D se $mdc(a, b) = 1$, ou equivalentemente, os únicos divisores comuns de a e b são os inversíveis.

Definição 31. Sejam D um domínio de integridade e $p \in D - \{0\}$, com $p \notin U(D)$. Dizemos que p é um elemento irredutível em D se para $x, y \in D$ vale a implicação: $p = xy \implies x \in U(D)$ ou $y \in U(D)$.

Um comentário pertinente a respeito de elementos irredutíveis é a seguinte.

Observação 13. *Seja D um domínio de integridade. Então, valem:*

i) Se x é um elemento irredutível de D e $y \in D$ é tal que x não divide y, então x e y são relativamente primos;

ii) Dados $x, y \in D$ nem sempre existe um mdc de x e y. Entretanto, se existe um mdc de x e y ele é único a menos de associados, isto é, se d e d' são dois mdc's de x e y, então $d \sim d'$.

Passemos então ao conceito de domínio de fatoração única.

Definição 32. Seja D um domínio de integridade. Dizemos que D é um DFU se as seguintes condições são satisfeitas:

i) Dado $a \in D - U(D)$, com $a \neq 0$, podemos fatorar a como um produto de elementos irredutíveis, ou seja, existem $p_1, ..., p_n$ elementos irredutíveis de D tais que $a = p_1...p_n$;

ii) Se $p_1, ..., p_n, q_1, ..., q_m \in D$ são elementos irredutíveis tais que $p_1...p_n = q_1...q_m$, então $n = m$ e $p_i \sim q_i$, para todo $i = 1, 2, ..., n$ (reordenando, se necessário).

Neste ponto gostaríamos de destacar que em determinados $DFU's$ a condição de dois elementos serem relativamente primos nos dá uma propriedade bastante útil, conforme mostra a observação a seguir.

Observação 14. *Sejam D um DFU tal que todo ideal de D é principal, e $x, y \in D$ com $mdc(x, y) = 1$. Então, existem $r, s \in D$, tais que $xr + ys = 1$.*

Para finalizarmos esta seção iremos definir o corpo de frações de um DFU. Sendo D um DFU consideremos o seguinte conjunto

$$K_D = \left\{ \frac{a}{b} \ / \ a, b \in D \text{ e } b \neq 0 \right\}$$

de modo que $\frac{a}{b} = \frac{c}{d}$ se, e somente se, $ad = bc$. Definamos as operações de adição e multiplicação em K_D, dadas respectivamente por

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd} \quad \text{e} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \ .$$

Temos que $(K_D, +, \cdot)$ é um corpo, chamado de corpo de frações do DFU D.

Observemos que a função $f : D \longrightarrow K_D$, dada por $f(a) = \frac{a}{1}$ é um homomorfismo injetivo de anéis, e assim $d \simeq Im\, f$. Além disso, identificando $a \in D$ com $\frac{a}{1} \in K_D$, podemos ver D como um subanel de K_D.

1.3 Corpos

1.3.1 Corpos e Subcorpos

Nesta seção iremos relembrar os conceitos de corpos e subcorpos. Além disso, destacaremos os resultados acerca destes conceitos que serão relevantes no decorrer deste trabalho. Indicamos as referências [3], [4] e [12] para as demonstrações dos resultados apresentados nesta seção, bem como para um leitor interessado em um estudo minucioso dos conceitos e ideias que apresentaremos a seguir.

Inicialmente, recordemos que um corpo é um anel comutativo com unidade no qual todo elemento não nulo é inversível. Observemos que, uma vez que corpos são casos particulares de anéis todos os resultados apresentados na Seção 1.2 continuam sendo válidos, embora como as condições necessárias para que um determinado anel seja um corpo são bastante exigentes, nem todos os resultados válidos para corpos continuam sendo válidos para anéis em geral.

Observemos também que todo corpo é um domínio de integridade, mas nem todo domínio de integridade é um corpo.

Recordemos também o conceito de subcorpos.

Definição 33. Sejam K um corpo e $\emptyset \neq L \subseteq K$. Dizemos que L é um subcorpo de K, e denotamos por $L \subseteq K$, se L satisfaz:

i) L é um subanel de K;

ii) $1_K \in L$ e $x^{-1} \in L$, para todo $x \in L - \{0\}$.

Observa-se que se L é um subcorpo de um corpo K, então L é por si um corpo. Ademais, se $L \neq K$, diremos que L é um subcorpo próprio de K.

O conceito de subcorpo próprio nos remete diretamente a ideia de corpos primos.

Definição 34. Dizemos que um corpo K é um corpo primo se K não possui subcorpos próprios.

Antes de apresentarmos alguns exemplos de corpos e subcorpos, iremos revisitar o conceito de característica de um anel no caso em particular que o anel em questão é um corpo. Observemos que, ao contrário de anéis em geral, as opções para a característica de um corpo são bem mais restritas, conforme mostra o teorema a seguir.

Teorema 10. *Seja K um corpo. Então, valem:*

i) Se $L \leq K$, então $charL = charK$;

ii) $charK = 0$ ou $charK = p$, onde p é um número primo;

iii) Se K é um corpo finito, então $charK = p$, sendo p um número primo.

Vejamos agora alguns exemplos de subcorpos.

Exemplo 29. *Observemos que os conjuntos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, munidos de suas adição e multiplicação usuais, são corpos. Ademais, $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ e $char\ \mathbb{Q} = char\ \mathbb{R} = char\ \mathbb{C} = 0$. Além disso, observemos que $\mathbb{Q}$ é um corpo primo.*

Exemplo 30. *O anel $\mathbb{Z}_n$, apresentado na Seção 1.2 (vide Exemplo 27, página 31), é um corpo se, e somente se, n é um número primo. Ademais, observemos que $char\ \mathbb{Z}_p = p$ e que $\mathbb{Z}_p$ é um corpo primo.*

No próximo resultado veremos que as possibilidades para a ordem de um corpo são mais restritas do que as possíveis ordens de um anel.

Teorema 11. *Se K é um corpo finito, então $|K| = p^n$, onde $p = charK$ e $n \in \mathbb{N}$. Ademais, para quaisquer $p, n \in \mathbb{N}$, com p um número primo, existe um corpo K tal que $|K| = p^n$.*

Para finalizarmos esta seção, veremos algumas observações importantes acerca de anéis de polinômios sobre um corpo.

Observação 15. *Sendo K um corpo, temos:*

i) $K[x]$ é um DFU no qual todo ideal é principal, isto é, se I é um ideal de $K[x]$, então existe $f(x) \in K[x]$ tal que $I =< f(x) >$;

ii) Todo ideal primo não nulo de $K[x]$ é um ideal maximal;

iii) $U(K[X])$ é o conjunto dos polinômios constantes e não nulos;

iv) Todo polinômio de grau 1 é irredutível em $K[x]$;

v) Se K é um corpo finito, então para todo $n \in \mathbb{N}$ existe um polinômio irredutível $f(x) \in K[x]$, tal que $\partial f(x) = n$.

1.3.2 Extensões de Corpos

Nesta seção iremos definir os conceitos de raízes de polinômios sobre corpos, extensões de corpos, extensões algébricas e extensões transcendentes. Além disso, destacaremos os resultados acerca destes conceitos que serão relevantes no decorrer deste trabalho. Para os leitores, interessados em um estudo mais aprofundado destes conceitos, indicamos as referências [3], [4] e [12].

Definição 35. Diremos que um corpo L é uma extensão de um corpo K (ou que $K \subseteq L$ é uma extensão de corpos), e denotaremos por $K \subseteq L$ ou L/K, se K for um subcorpo de L.

Sendo L/K uma extensão de corpos, consideremos a adição de L e o seguinte produto por escalar

$$\begin{aligned} \cdot : \ K \times L &\longrightarrow L \\ (\lambda, x) &\longmapsto \lambda \cdot x \end{aligned}$$

onde $\lambda \cdot x$ é o produto de λ por x no corpo L. Temos que L, munido dessas operações é um K-espaço vetorial. A dimensão de L como K-espaço vetorial, a qual é denotada por $[L : K]$, é chamada de *grau da extensão* L/K.

Diremos que L/K é uma extensão finita se $[L : K]$ for finito, caso contrário, diremos que L/K é uma extensão infinita.

Passemos agora ao estudo de extensões geradas por um conjunto. Seja L uma extensão de um corpo K e S um subconjunto de L. Definimos o subcorpo de L gerado por K e S (ou a subextensão de L/K gerada por S) como sendo a interseção de todos os subcorpos de L que contém K e S. Denotamos o subcorpo de L gerado por K e S por $K(S)$. Sendo $S = \{a_1, ...a_n\}$ um conjunto finito, normalmente denotamos $K(S)$ por $K(a_1, ..., a_n)$.

Diremos que uma extensão L/K é uma *extensão finitamente gerada* se existe um subconjunto S de L tal que $L = K(S)$. Ademais, no caso particular em que S é um conjunto unitário diremos que a extensão L/K é uma *extensão simples*.

Um comentário pertinente a respeito de extensões finitas é o fato de que se K é um corpo finito e L é uma extensão finita de K, então L é um corpo finito.

Definição 36. Sejam L uma extensão de um corpo K e $a \in L$. Diremos que a é rais de um polinômio $f(x) \in K[x]$, se $f(a) = 0$. Diremos também que a é algébrico sobre K se existir algum polinômio não nulo $f(x) \in K[x]$ tal que a é raiz de $f(x)$. Caso contrário, diremos que a é transcendente sobre K.

Diremos que L é uma *extensão algébrica* de K se todo elemento de L for algébrico sobre K. Caso contrário, diremos que L é uma *extensão transcendente* de K.

Sejam L uma extensão de um corpo K e $a \in L$. Consideremos a seguinte função

$$\begin{aligned} \psi_a : \ & K[x] \longrightarrow L \\ & f(x) \longmapsto \psi_a(f(x)) = f(a) \end{aligned}$$

Temos que ψ_a é um homomorfismo de anéis. Ademais, observemos que $Im\ \psi_a = \{f(a)\ /\ f(x) \in K[x]\}$ e iremos denotar $Im\ \psi_a$ simplesmente por $K[a]$. Observemos também que $K[a]$ é um subanel de K.

Notemos agora que se a é um elemento transcendente sobre K, então $Ker\ \psi_a = \{f(x) \equiv 0\}$, onde $f(x) \equiv 0$ denota o polinômio identicamente nulo. Assim, pelo Teorema Fundamental dos Homomorfismos (vide Teorema 8, página 33), temos que $K[x] \simeq K[a]$.

Por outro lado, sendo a algébrico sobre K, temos que $Ker\ \psi_a$ é um ideal primo não nulo. Neste caso, $Ker\ \psi_a$ é um ideal maximal de $K[x]$. Portanto, uma vez que $K[x]$ é um domínio de integridade (recordemos que $K[x]$ é um DFU), temos que $\frac{K[x]}{Ker\ \psi_a}$ é um corpo (veja Teorema 7, página 32), e como pelo Teorema Fundamental do Homomorfismos (veja Teorema 8, página 33) temos $\frac{K[x]}{Ker\ \psi_a} \simeq K[a]$, segue que $K[a]$ é um corpo. Observemos que neste caso $K[a] = K(a)$.

Observação 16. *Toda extensão finita de corpos é algébrica.*

Definiremos agora fecho algébrico de um corpo. Entretanto, para isso necessitamos da definição de corpos algebricamente fechados.

Definição 37. Seja K um corpo. Dizemos que K é um um corpo algebricamente fechado se todo polinômio não constante $f(x) \in K[x]$ possui raiz em K.

Uma observação a respeito de corpos algebricamente fechados é que se K é um corpo, então existe alguma extensão de K que é algebricamente fechada.

Agora, de posse do conceito de corpo algebricamente fechado, passemos à definição de fecho algébrico de um corpo.

Definição 38. Seja K um corpo. Definimos um fecho algébrico de K, e denotamos por $\overline{K}$, como sendo uma extensão algébrica de K que é algebricamente fechada.

Observemos que todo corpo K possui fecho algébrico. Além disso, fazendo uso do Teorema da Extensão do Isomorfismo (enunciado a seguir), é possível mostrar que o fecho algébrico de um corpo é único a menos de isomorfismo, isto é, se K é um corpo e F_1 e F_2 são dois fechos algébricos de K, então $F_1 \simeq F_2$.

Teorema 12 (**Teorema da Extensão do Isomorfismo**). *Sejam K um corpo e F uma extensão algébrica de K. Se L é um corpo algebricamente fechado e $\sigma : K \longrightarrow L$ é uma imersão (homomorfismo injetivo), então existe uma imersão $\sigma_1 : F \longrightarrow L$ estendendo σ.*

Capítulo 2

Grupos Aditivos e Multiplicativos de Anéis

Neste capítulo iremos estudar algumas propriedades de grupos aditivos e multiplicativos de anéis, como também, buscando compreender melhor essas estruturas algébricas, faremos uma descrição detalhada da estrutura dos grupos multiplicativos de alguns anéis clássicos. Finalizaremos este capítulo fazendo um estudo dos grupos de ordem menor ou igual a 11 no sentido de determinar quais desses grupos são grupos multiplicativos de algum anel.

2.1 Considerações Iniciais

Inicialmente, definiremos os conceitos de grupo aditivo e grupo multiplicativo de um anel.

Definição 39. Sendo $(R, +, \cdot)$ um anel, definimos o grupo aditivo do anel R como sendo $(R, +)$, ou seja, o conjunto R munido da adição.

Segue da definição de anel (vide Definição 17, página 25) que $(R, +)$ é realmente um grupo e é abeliano.

Consideremos agora R um anel com unidade e $U(R)$ o conjunto dos elementos inversíveis de R. Sendo $a, b \in U(R)$, observemos que

$$(b^{-1}a^{-1})(ab) = (ab)(b^{-1}a^{-1}) = 1_R$$

e assim $ab \in U(R)$ e $(ab)^{-1} = b^{-1}a^{-1}$. Observemos também que $a^{-1} \in U(R)$ e $(a^{-1})^{-1} = a$.

Como $U(R)$ é multiplicativamente fechado, podemos considerar a multiplicação como uma operação em $U(R)$ (restrição da multiplicação a $U(R)$). Ademais, $(U(R), \cdot)$ é um grupo e assim temos a seguinte definição.

Definição 40. Sendo $(R, +, \cdot)$ um anel, definimos o grupo multiplicativo do anel R como sendo $(U(R), \cdot)$, ou seja, o conjunto $U(R)$ munido da multiplicação.

Fixemos algumas notações que serão utilizadas ao longo deste capítulo. Sendo R um anel, $(R, +)$ irá denotar o seu grupo aditivo. Além disso, se R possui unidade $U(R)$ irá denotar o seu grupo multiplicativo.

Observa-se facilmente que se R é um anel comutativo com unidade, então $U(R)$ é um grupo abeliano. No entanto, a recíproca não é válida. De fato, considerando K um corpo de 2 elementos e o subanel

$$U_2(K) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \ / \ a, b \text{ e } c \in K \right\}$$

de $M_2(K)$, temos que $U_2(K)$ é um anel com unidade não comutativo e no entanto o seu grupo multiplicativo tem apenas 2 elementos, sendo portanto abeliano.

Recordemos que na introdução deste trabalho, foram levantadas as seguintes questões:

• Dado um grupo abeliano G é possível definir uma operação de multiplicação que o torne um anel?

• Dado um grupo G existe algum anel cujo grupo multiplicativo seja isomorfo a G?

Observemos que, à primeira vista, a primeira dessas perguntas pode ser respondida facilmente. De fato, sendo $(G, *)$ um grupo abeliano consideremos a seguinte operação:

$$\begin{aligned} \cdot : \ & G \times G \longrightarrow G \\ & (g, h) \longmapsto g \cdot h = e \end{aligned}$$

onde e é o elemento neutro de $(G, *)$. Com alguns cálculos diretos pode-se verificar que $(G, *, \cdot)$ é um anel. Assim, todo grupo abeliano é grupo aditivo de algum anel.

Entretanto, podemos particularizar essa questão, bastando exigirmos um pouco mais do anel, como, por exemplo, que o anel seja um anel com unidade, ou um domínio de integridade. Observemos que essas particularizações tornam a questão mais enriquecedora, embora, tendo em vista a diversidade de anéis, nesses formatos esta questão é muito mais delicada e difícil de se responder.

Apresentaremos agora um exemplo de grupo que não é grupo multiplicativo de nenhum anel com unidade. Para isso, precisamos do seguinte resultado.

Teorema 13. *Seja R um anel com unidade. Se $(R,+)$ é um grupo de torção, então $exp\ (R,+)$ é finito.*

Demonstração. Sendo $(R,+)$ um grupo de torção, então $o(1_R)$ é finita, digamos $o(1_R) = n$. Assim, dado $x \in R$ temos

$$nx = n(1_R x) = (n1_R)x = 0x = 0.$$

Logo, $nx = 0$ para todo $x \in R$, e portanto $exp\ (R,+)$ é finito. □

Recordemos agora que, conforme comentamos no Exemplo 13, o grupo $\frac{\mathbb{Q}}{\mathbb{Z}}$ é um grupo de torção, embora não seja um grupo de expoente finito. Assim, pelo Teorema 13, temos que o grupo $\frac{\mathbb{Q}}{\mathbb{Z}}$ não é grupo multiplicativo de nenhum anel com unidade.

Mostremos agora um teorema que, apresentando uma condição necessária para que determinado anel seja um domínio de integridade, nos possibilita encontrar diversos exemplos de grupos que não são grupos multiplicativos de domínio de integridade.

Contudo, antes de apresentarmos este teorema, gostaríamos de observar que se R é um anel tal que $charR = n > 0$, então é imediato que n é exatamente o expoente do grupo $(R,+)$. Passemos então ao teorema.

Teorema 14. *Se R é um domínio de integridade, então $charR = 0$ ou $charR = p$, onde p é um número primo.*

Demonstração. Suponhamos $charR \neq 0$. Assim, $charR = n$, com $n \in \mathbb{N}$.

Sendo $charR = n$, temos que $n = min\{k \in \mathbb{N} \,/\, k1_R = 0\}$. Supondo n não primo, podemos tomar $n_1, n_2 \in \mathbb{N}$ tais que $n = n_1 n_2$ e ainda $1 < n_1, n_2 < n$. Daí, devemos ter $0 = n1_R = (n_1 1_R)(n_2 1_R)$. Mas, sendo R um $D.I.$, devemos ter $(n_1 1_R) = 0$ ou $(n_2 1_R)$, mas isto é um absurdo, uma vez que $n_1, n_2 < n$ e $charR = n$. Logo, $charR = p$, com p primo. □

Uma vez que se $charR = exp(R,+) = n$ (se $charR > 0$), se G é um grupo tal que $exp\, G = n$, com n um número não primo, então do Teorema 14, temos que G não é grupo multiplicativo de nenhum domínio de integridade.

Em relação à segunda questão colocada no início da seção, iremos abordá-la com maiores detalhes nas próximas seções.

Um fato importante que gostaríamos de destacar é que, embora os grupos aditivo e multiplicativo de um anel sejam estruturas algébricas distintas, em casos particulares, propriedades do grupo aditivo de um anel afetam diretamente a estrutura multiplicativa do anel em questão. Para maior compreensão desse fato, observemos o teorema a seguir.

Teorema 15. *Se R é um anel tal que $(R,+)$ é cíclico, então R é um anel comutativo.*

Demonstração. Sendo $(R,+)$ cíclico, digamos $(R,+) =< a >$, dados $x, y \in R$ existem $n, m \in \mathbb{Z}$ tais que $x = na$ e $y = ma$. Assim,

$$xy = (na)(ma) = (nm)a = (mn)a = (ma)(na) = yx$$

e portanto R é um anel comutativo. □

Entretanto, a condição de que R seja um anel cujo grupo aditivo é cíclico é bastante exigente e apenas poucos anéis a satisfazem. Por exemplo, se acrescentarmos a essa condição a hipótese de que R seja um anel com unidade, temos, a menos de isomorfismo, apenas os anéis $\mathbb{Z}$ e $\mathbb{Z}_n$ satisfazendo essas duas condições simultaneamente, conforme mostra o teorema a seguir.

Teorema 16. *Seja R um anel com unidade tal que $(R,+)$ é cíclico. Então, $R \simeq \mathbb{Z}$ ou $R \simeq \mathbb{Z}_n$, para algum $n \in \mathbb{N}$.*

Demonstração. Sendo R um anel com unidade tal que $(R,+)$ é cíclico, digamos $(R,+) =< a >= \{ma \ / \ m \in \mathbb{Z}\}$, consideremos a aplicação

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow R \\ m &\longmapsto f(m) = ma \end{aligned}$$

Observemos que f é um homomorfismo sobrejetivo de anéis. De fato, a sobrejetividade de f segue de $(R,+) =< a >$, e dados $n, m \in \mathbb{Z}$, temos

$$f(n+m) = (n+m)a = na + ma = f(n) + f(m)$$

e

$$f(nm) = (nm)a = (na)(ma) = f(n)f(m)$$

Ademais, se R é um anel infinito, devemos ter $o(a) = \infty$ (em $(R,+)$), e daí $Ker f = \{m \in \mathbb{Z} \ / \ ma = 0_R\} = \{0\}$. Portanto, f é injetiva (vide Observação 12, página 32), donde decorre $\mathbb{Z} \simeq R$.

Por outro lado, se R é um anel finito digamos $|R| = n$, devemos ter $o(a) = n$ e daí $Ker f = \{m \in \mathbb{Z} \ / \ ma = 0_R\} = m\mathbb{Z}$ (vide Observação 3, página 16). Logo, pelo Teorema Fundamental dos Homomorfismos (vide Teorema 8, página 33), temos que $\mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}} \simeq R$. □

Para finalizar esta seção, iremos reforçar que a diversidade de estruturas de anéis que aparecem na literatura clássica dificulta o estudo das propriedades de grupos aditivos e multiplicativos de anéis. A título de ilustração apresentaremos agora uma propriedade de grupos aditivos e multiplicativos de anéis sobre a qual nada se pode concluir num caráter mais geral.

Sendo R um anel finito (com unidade), temos que os grupos aditivo, e multiplicativo de R são finitos e portanto finitamente gerados. Mostremos

agora que se R for um anel infinito,sozinha esta informação não nos permite concluir nada sobre finitude ou infinitude de conjuntos geradores de seus grupos aditivo e multiplicativo. De fato, notemos que $(\mathbb{Z}, +)$ é um grupo infinito e cíclico ($(\mathbb{Z}, +) =< 1 >$). Entretanto, $(\mathbb{Q}, +)$ é um grupo infinito, mas na Seção 3.1 demonstraremos que $(\mathbb{Q}, +)$ não é nem finitamente gerado.

O mesmo ocorre para os grupos multiplicativos de $\mathbb{Z}$ e $\mathbb{Q}$: $U(\mathbb{Z})$ é um grupo cíclico, a saber, $U(\mathbb{Z}) = \{-1, 1\} =< -1 >$. Entretanto, na Seção 3.2, iremos mostrar que $U(\mathbb{Q})$ não é nem finitamente gerado.

2.2 Grupos Multiplicativos de Alguns Anéis Clássicos

Buscando evitar as complicações causadas pela diversidade das estruturas dos anéis existentes, nesta seção iremos estudar casos bastantes particulares de grupos multiplicativos de anéis. Destacamos que, embora ao restringirmos esse estudo para apenas alguns anéis percamos a generalidade, em contrapartida essa restrição nos garante um maior entendimento das estruturas algébricas envolvidas nesse estudo. Assim, nesta seção faremos uma descrição detalhada da estrutura dos grupos multiplicativos de alguns anéis clássicos e bastante recorrentes na literatura, como também destacaremos as propriedades decorrentes destas descrições.

2.2.1 Grupo multiplicativo do anel $\mathbb{Z}_n$

Iniciaremos esse estudo, descrevendo a estrutura do grupo multiplicativo do anel $\mathbb{Z}_n$, com $n \in \mathbb{N}$, o qual foi apresentado no Exemplo 27. Entretanto, antes dessa descrição, apresentaremos alguns resultados, bem como algumas propriedades básicas de $U(\mathbb{Z}_n)$ que nos serão imprescindíveis no decorrer desta seção.

Observemos que se $\overline{a} \in U(\mathbb{Z}_n)$, então existe $\overline{b} \in U(\mathbb{Z}_n)$ tal que $\overline{a}\overline{b} = \overline{1}$, ou seja, $ab \equiv 1(mod\ n)$ e portanto $ab - kn = 1$ com $k \in \mathbb{Z}$. Mas isto ocorre somente se $mdc(a, n) = 1$. Por outro lado, supondo $mdc(a, n) = 1$, temos que existem $r, s \in \mathbb{Z}$ tais que $ar + ns = 1$, ou seja, $ar - 1 = -ns$ e portanto $ar \equiv 1(mod\ n)$, donde segue que $\overline{ar} = \overline{a} \cdot \overline{r} = \overline{1}$. Logo, $\overline{a} \in U(\mathbb{Z}_n)$. Assim, podemos concluir que $U(\mathbb{Z}_n) = \{\overline{a} \in \mathbb{Z}_n \ ; \ mdc(a, n) = 1\}$. Ademais, uma vez que a função φ de Euler aplicada a n conta exatamente os números m tais que $mdc(n, m) = 1$ e $0 \leq m < n$, obtemos que $|U(\mathbb{Z}_n)| = \varphi(n)$.

Um outro resultado necessário para a técnica que utilizaremos para descrever a estrutura de $U(\mathbb{Z}_n)$ consiste num teorema que, em determinadas condições, nos permite decompor o anel $\mathbb{Z}_n$ em produto direto.

Teorema 17. *Se $mdc(n,m) = 1$, então os anéis $\mathbb{Z}_{mn}$ e $\mathbb{Z}_m \times \mathbb{Z}_n$ são isomorfos.*

Demonstração. Inicialmente, observemos que, como $mdc(n,m) = 1$, devemos ter $mmc(m,n) = mn$. Consideremos agora a aplicação

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n \\ k &\longmapsto f(k) = (\overline{k}, \overline{\overline{k}}) \end{aligned}$$

onde $\overline{k}$ e $\overline{\overline{k}}$ denotam as classes de congruência de k $(mod\ m)$ e $(mod\ n)$, respectivamente.

Observa-se facilmente das propriedades de congruência modular que f é um homomorfismo de anéis. Ademais, dado $(\overline{a}, \overline{\overline{b}}) \in \mathbb{Z}_m \times \mathbb{Z}_n$, mostremos que existe $k \in \mathbb{Z}$ tal que $f(k) = (\overline{a}, \overline{\overline{b}})$. De fato, como $mdc(m,n) = 1$, existem $r, t \in \mathbb{Z}$ tais que $1 = mr + nt$. Assim, tomando $k = bmr + ant$ temos

$$\begin{aligned} \overline{k} &= \overline{bmr + ant} \\ &= \overline{bmr} + \overline{ant} \\ &= \overline{ant} \\ &= \overline{a(1 - mr)} \\ &= \overline{a} - \overline{amr} \\ &= \overline{a} \end{aligned}$$

Analogamente, mostra-se que $\overline{\overline{k}} = \overline{\overline{b}}$. Logo, $f(k) = (\overline{a}, \overline{\overline{b}})$ e portanto f é sobrejetiva.

Notemos também que $Ker f = \{k \in \mathbb{Z} \ ; \ n \text{ e } m \text{ dividem } k\}$ e como $mmc(m,n) = mn$, devemos ter $Ker f = mn\mathbb{Z}$. Daí, pelo Teorema Fundamental dos Homomorfismos (vide Teorema 8, página 33), segue que

$$\frac{\mathbb{Z}}{mn\mathbb{Z}} = \mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n \ .$$

□

Neste ponto destacamos que, utilizando-se o princípio de indução, podemos generalizar o Teorema 17 obtendo-se o teorema a seguir.

Teorema 18. *Se $n_1, n_2, ..., n_k \in \mathbb{N}$ são dois a dois relativamente primos, então os anéis $\mathbb{Z}_{n_1 n_2 ... n_k}$ e o produto direto $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_k}$ são isomorfos.*

Consideremos agora o anel $\mathbb{Z}_m$ e recordemos que podemos decompor m em produto de potências de primos do seguinte modo: $m = p_1^{a_1} p_2^{a_2} ... p_n^{a_n}$,

onde $p_1, p_2, ..., p_n$ são primos dois a dois distintos e $a_i \in \mathbb{N}$. Assim, como $mdc(p_i^{a_i}, p_j^{a_j}) = 1$, para $i \neq j$, pelo Teorema 18 temos

$$\mathbb{Z}_m = \mathbb{Z}_{p_1^{a_1} p_2^{a_2} ... p_n^{a_n}} \simeq \mathbb{Z}_{p_1^{a_1}} \times ... \times \mathbb{Z}_{p_n^{a_n}}.$$

Recordemos também que se $R_1, R_2, ..., R_n$ são anéis com unidade vale $U(R_1 \times R_2 \times, ..., \times R_n) \simeq U(R_1) \times U(R_2) \times ... \times U(R_n)$. Assim, para descrevermos a estrutura de $U(\mathbb{Z}_m)$ é necessário apenas que descrevamos a estrutura de cada $U(\mathbb{Z}_{p_i^{a_i}})$ e apliquemos o Teorema 18.

Apresentaremos agora uma descrição de $U(\mathbb{Z}_{p^k})$, como feita em [11], para todo p primo e $k \in \mathbb{N}$. Dividiremos em dois casos, p ímpar e $p = 2$. Porém, antes desta descrição, destaquemos a seguinte observação: se K é um corpo finito, então $U(K)$ é cíclico (mostraremos esse fato na Seção 3.2 e o usaremos largamente nesta seção).

Enunciaremos agora dois lemas que serão bastante úteis no decorrer desta seção. Estes lemas tratam de congruência modular, e para um leitor mais curioso a respeito de propriedades da aritmética modular aconselhamos consultar a referência [7].

Lema 1. *Para todo $m \in \mathbb{Z}$ com $m \geq 0$, temos $(1+p)^{p^m} \equiv 1 (mod\ p^{m+1})$ e além disso, $(1+p)^{p^m} \not\equiv 1 (mod\ p^{m+2})$.*

Demonstração. Faremos a demonstração por indução em m. Para $m = 0$ temos $(1+p) \equiv 1 (mod\ p)$ e $(1+p) \not\equiv 1 (mod\ p^2)$ e o resultado é válido. Para $m = 1$, temos

$$(1+p)^p = \sum_{j=0}^{p} \binom{p}{j} p^j = 1 + p^2 + p^3(\tfrac{p-1}{2}) + ... + p^p$$

assim, temos que $(1+p)^p - 1$ é múltiplo de p^2, mas não de p^3.

Consideremos agora $a = (1+p)^{p^m}$ e suponhamos por indução que o resultado vale para $m = k \geq 1$, ou seja, $a = (1+p)^{p^k} \equiv 1 (mod\ p^{k+1})$ e também $(1+p)^{p^k} \not\equiv 1 (mod\ p^{k+2})$. Observemos que $(1+p)^{p^{k+1}} = a^p$ e também que $a^p - 1 = (a-1) \sum_{j=0}^{p-1} a^j$.

Assim, uma vez que $a \equiv 1 (mod\ p^{k+1})$, segue que $a^s \equiv 1 (mod\ p^{k+1})$, para todo $s \in \mathbb{N}$. Portanto, temos

$$\frac{a^p - 1}{a - 1} = \sum_{k=0}^{p-1} a^k = a^{p-1} + ... + a + 1 \equiv p\ (mod\ p^{k+1}).$$

Donde, p divide $\frac{a^p-1}{a-1}$, mas p^2 não divide $\frac{a^p-1}{a-1}$ (pois $k+1 \geq 2$).

Como $a^p - 1 = \frac{a^p-1}{a-1}(a-1)$, p^{k+1} divide $a-1$ e p^{k+2} não divide $a-1$, temos que p^{k+2} divide a^p-1 e p^{k+3} não divide a^p-1.

Logo,

$$a^p \equiv 1 \ (mod\ p^{k+2}) \quad \text{e} \quad a^p \not\equiv 1 \ (mod\ p^{k+3}),$$

ou seja,

$$(1+p)^{p^{k+1}} \equiv 1 \ (mod\ p^{k+2}) \quad \text{e} \quad (1+p)^{p^{k+1}} \not\equiv 1 \ (mod\ p^{k+3}),$$

e temos o resultado. □

Lema 2. *Para todo $k \in \mathbb{N}$, com $k \geq 3$, vale $5^{2^{k-3}} \equiv 1 + 2^{k-1}(mod\ 2^k)$.*

Demonstração. Faremos a demonstração por indução em k. Para $k = 3$ temos

$$5^{2^{3-3}} = 5 \equiv 5 = 1 + 2^{3-1}(mod\ 2^3).$$

Suponhamos então, por hipótese de indução, que o resultado vale para $k = m \geq 3$, isto é, que vale $5^{2^{m-3}} \equiv 1 + 2^{m-1}(mod\ 2^m)$, e mostremos que $5^{2^{m-2}} \equiv 1 + 2^m(mod\ 2^{m+1})$.

Para tal consideremos $a = 5^{2^{m-3}}$. Daí $a^2 = 5^{2^{m-2}}$ e observemos que, por hipótese de indução, vale $a \equiv 1 + 2^{m-1}(mod\ 2^m)$, donde segue que $2a \equiv 2 + 2^m(mod\ 2^{m+1})$ e portanto $2a - 1 \equiv 1 + 2^m(mod\ 2^{m+1})$.

Por outro lado, como $a \equiv 1 + 2^{m-1}(mod\ 2^m)$, temos que 2^m divide $(a-1) - 2^{m-1}$. Assim, uma vez que 2^{m-1} divide 2^m, temos que 2^{m-1} divide $(a-1) - 2^{m-1}$, e portanto 2^{m-1} divide $(a-1)$. Logo, $(2^{m-1})^2$ divide $(a-1)^2$, e daí, 2^{m+1} divide $a^2 - 2a + 1$ (pois $m + 1 \leq 2m - 2$), o que implica $a^2 \equiv 2a - 1(mod\ 2^{m+1})$. Assim, como $2a - 1 \equiv 1 + 2^m(mod\ 2^{m+1})$, temos $a^2 = 5^{2^{m-2}} \equiv 1 + 2^m(mod\ 2^{m+1})$ e o resultado segue. □

Teorema 19. *Seja p um número primo ímpar. Então, o grupo multiplicativo $U(\mathbb{Z}_{p^n}) = \{\overline{a} \in \ \mathbb{Z}_{p^n} \ / \ mdc(a,p) = 1\}$ é cíclico de ordem $(p-1)p^{n-1}$.*

Demonstração. Inicialmente, notemos que se $n = 1$, então $\mathbb{Z}_p$ é um corpo e daí $U(\mathbb{Z}_p)$ é cíclico com $|U(\mathbb{Z}_p)| = p - 1$.

Supondo agora $n \geq 2$, temos $|U(\mathbb{Z}_{p^n})| = \varphi(p^n) = (p-1)p^{n-1}$, onde φ denota a função φ de Euler. Consideremos $B = \{\overline{b} \in U(\mathbb{Z}_{p^n}) \ / \ b \equiv 1(mod\ p)\}$. Temos $\overline{1} \in B$, e dados $\overline{x}, \overline{y} \in B$ devemos ter $x \equiv 1(mod\ p)$ e $y \equiv 1(mod\ p)$, donde $xy \equiv 1(mod\ p)$ e assim $\overline{xy} \in B$. Assim, como B é finito e fechado à operação, como visto no Exemplo 6 temos que B é um subgrupo de $U(\mathbb{Z}_n)$.

Notemos que cada inteiro $b \in \{0, 1, ..., p^n - 1\}$ pode ser escrito com uma expressão única do seguinte modo:

$$b = a_0 + a_1 p + ... + a_{n-1} p^{n-1}$$

onde $0 \leq a_i \leq p$, para todo $i = 0, 1, ..., n-1$, e assim

$$\overline{\overline{b}} = \overline{\overline{a_0 + a_1 p + ... + a_{n-1} p^{n-1}}} = \overline{\overline{a_o}}$$

onde $\overline{\overline{b}}$ denota a classe de congruência $(mod\ p)$ de b. Logo, dado $\overline{b} \in U(\mathbb{Z}_{p^n})$ (com $0 \leq b < p^n$), temos $\overline{b} \in B$ se, e somente se, quando escrevermos b na decomposição anterior tivermos $a_0 = 1$. Daí, pelo princípio multiplicativo temos $|B| = p^{n-1}$.

Como a recíproca do Teorema de Lagrange é válida para grupos abelianos, existe $A \leq U(\mathbb{Z}_{p^n})$ tal que $|A| = p - 1$ e daí, como $mdc(|A|, |B|) = 1$, segue do Corolário 1 que $A \cap B = \{\overline{1}\}$. Assim, $|AB| = (p-1)p^{n-1} = |U(\mathbb{Z}_{p^n})|$, e portanto $AB = U(\mathbb{Z}_{p^n})$.

Neste ponto destacamos que para mostrar que $U(\mathbb{Z}_{p^n})$ é um grupo cíclico, é suficiente mostrar que A e B são cíclicos (veja Teorema 3, página 20). Mostremos então que A é um grupo cíclico, e para tal consideremos a função

$$\begin{aligned} f : U(\mathbb{Z}_{p^n}) &\longrightarrow U(\mathbb{Z}_p) \\ (\overline{a}) &\longmapsto f(\overline{a}) = \overline{\overline{a}} \end{aligned}$$

Inicialmente, observemos que f é bem definida, pois se $\overline{a} = \overline{b}$, então $a \equiv b(mod\ p^n)$, ou seja, $a - b = kp^n$ e portanto $a - b = (kp^{n-1})p$, isto é, $a \equiv b(mod\ p)$. Logo $\overline{\overline{a}} = \overline{\overline{b}}$. Ademais, f é um homomorfismo de grupos. De fato, dados $\overline{a}$, $\overline{b} \in U(\mathbb{Z}_{p^n})$, temos

$$\begin{aligned} f(\overline{ab}) &= \overline{\overline{ab}} \\ &= \overline{\overline{a}}\,\overline{\overline{b}} \\ &= f(\overline{a}) f(\overline{b}) \end{aligned}$$

Observemos agora que dado $\overline{\overline{b}} \in U(\mathbb{Z}_p)$, temos $b \equiv k(mod\ p)$ para algum $0 \leq k \leq p-1$, e daí temos $\overline{\overline{b}} = \overline{\overline{k}} = f(\overline{k})$. Logo, f é um homomorfismo sobrejetivo de grupos. Além disso, temos $Ker f = B$, pela própria maneira como definimos B, e portanto do Teorema Fundamental dos Homomorfismos (vide Teorema 4, página 23) segue que $\frac{U(\mathbb{Z}_{p^n})}{B} \simeq U(\mathbb{Z}_p) \simeq C_{p-1}$.

Por outro lado, como $U(\mathbb{Z}_{p^n}) = AB$, do Segundo Teorema de Isomorfismo (vide Teorema 5, página 24) temos que

$$\frac{U(\mathbb{Z}_{p^n})}{B} = \frac{AB}{B} \simeq A$$

pois $A \cap B = \{\overline{1}\}$. Assim, $A \simeq \mathbb{Z}_{p-1}$ e portanto A é cíclico.

Mostremos agora que B é cíclico, observando que $B =< \overline{1+p} >$. Para tal, observemos que, tomando $m = n-1$ e depois $m = n-2$ no Lema 1, temos $(1+p)^{p^{n-1}} \equiv 1(mod\ p^n)$ e $(1+p)^{p^{n-2}} \not\equiv 1(mod\ p^n)$, respectivamente. Assim, $\overline{1+p}^{p^{n-1}} = \overline{1}$, mas $\overline{1+p}^{p^{n-2}} \neq \overline{1}$ em $U(\mathbb{Z}_{p^n})$, donde $o(\overline{1+p})$ divide p^{n-1}, mas não divide p^{n-2}. Logo, $o(\overline{p+1}) = p^{n-1} = |B|$, e portanto $B =< \overline{1+p} >$, donde B é cíclico.

Logo, uma vez que $U(\mathbb{Z}_{p^n}) \simeq AB$, e A e B são cíclicos de ordens relativamente primas, segue do Teorema 3, que $U(\mathbb{Z}_{p^n})$ é cíclico e que vale $|U(\mathbb{Z}_{p^n})| = (p-1)p^{n-1}$.

□

Estudemos agora o caso em que $p = 2$.

Teorema 20. *Sejam $m \in \mathbb{N}$ e $U(\mathbb{Z}_{2^m})$ o grupo multiplicativo do anel $\mathbb{Z}_{2^m}$. Então, $U(\mathbb{Z}_{2^m}) = \{\overline{a} \in \mathbb{Z}_{2^m} \ / \ a \text{ é impar}\}$. Ademais, $U(\mathbb{Z}_2) = \{\overline{1}\}$, $U(\mathbb{Z}_4) \simeq C_2$ e se $m \geq 3$, devemos ter*

$$U(\mathbb{Z}_{2^m}) =< \overline{-1}, \overline{5} > \simeq C_2 \times C_{2^{m-2}}$$

Demonstração. Inicialmente, recordemos que $\overline{a} \in U(\mathbb{Z}_{2^m})$ se, e somente se, $mdc(a, 2^m) = 1$. Logo, $U(\mathbb{Z}_{2^m}) = \{\overline{a} \in \mathbb{Z}_{2^m} \ / \ a \text{ é ímpar}\}$ e temos a primeira parte do teorema. Uma outra informação que segue desta afirmação é que $|U(\mathbb{Z}_{2^m})| = 2^{m-1}$.

Observemos que no caso em que $m = 1$, teremos $\mathbb{Z}_{2^m} = \mathbb{Z}_2$, e portanto $U(\mathbb{Z}_{2^m}) = \{\overline{1}\}$. Se $m = 2$, então $\mathbb{Z}_{2^m} = \mathbb{Z}_4$, e portanto $U(\mathbb{Z}_{2^m}) = \{\overline{1}, \overline{3}\} \simeq C_2$.

Suponhamos então $m \geq 3$. Daí, como $|U(\mathbb{Z}_{2^m})| = \varphi(2^m) = 2^{m-1}$, onde φ é a função φ de Euler, segue do Corolário 1 que $|\overline{5}| = 2^s$, com $s \leq m-1$.

Notemos que, do Lema 2, temos $5^{2^{m-3}} \equiv 1 + 2^{m-1}(mod\ 2^m)$ e daí $\overline{5^{2^{m-3}}} = \overline{1+2^{m-1}} \neq \overline{1}$, em $\mathbb{Z}_{2^m}$. Assim, da Observação 3, segue que 2^{m-3} não divide $2^s = |\overline{5}|$. Logo, devemos ter $s \geq m-2$.

Provemos agora que devemos ter $< \overline{5} > \cap < \overline{-1} >= \{\overline{1}\}$. De fato, se $< \overline{5} > \cap < \overline{-1} >\neq \{\overline{1}\}$, deveríamos ter $\overline{5^t} = \overline{-1}$ para algum $t \in \mathbb{N}$. Entretanto, como $m \geq 3$ esta igualdade nos daria $5^t \equiv -1(mod\ 4)$. Porém $5 \equiv 1(mod\ 4)$ e daí $5^t \equiv 1(mod\ 4)$, mas isto nos daria um absurdo, uma vez que $-1 \not\equiv 1(mod\ 2^m)$. Logo, $< \overline{5} > \cap < \overline{-1} >= \{\overline{1}\}$.

Recordemos agora que em um grupo abeliano todo subgrupo é normal e portanto o produto de subgrupos é ainda um subgrupo (veja o Exemplo 7, página 18). Assim, considerando $N =< \overline{5} >< \overline{-1} >$, temos que $N \leq U(\mathbb{Z}_{2^m})$ e assim $N =< \overline{5}, \overline{-1} >$. Ademais, como $< \overline{5} > \cap < \overline{-1} >= \{\overline{1}\}$ temos

$$|N| = | < \overline{5} > || < \overline{-1} > | = 2 \cdot 2^s \geq 2 \cdot 2^{m-2} = |U(\mathbb{Z}_{2^m})|.$$

Logo, $N = U(\mathbb{Z}_{2^m})$ e $|\overline{5}| = 2^{m-2}$, e portanto

$$U(\mathbb{Z}_{2^m}) \simeq < \overline{5} > \times < \overline{-1} > \simeq C_2 \times C_{2^{m-2}}.$$

□

Assim, com a descrição de $U(\mathbb{Z}_{p^k})$ feita, para todo p primo e $k \in \mathbb{N}$, aplicando o teorema 18, temos imediatamente a descrição de $U(\mathbb{Z}_m)$.

2.2.2 Grupo Multiplicativo de End(G)

Sendo $G = (G, *)$ um grupo abeliano, consideremos $End(G)$ o conjunto de todos os endomorfismos de G, ou seja, o conjunto de todos os homomorfismos de G em G, e $Aut\ G$ o conjunto de todos os automorfismos de G, isto é, o conjunto de todos os isomorfismos de G em G. Para $\varphi,\ \psi \in End(G)$ definamos

$$\begin{aligned} \varphi + \psi : G &\longrightarrow G \\ x &\longmapsto (\varphi + \psi)(x) = \varphi(x) * \psi(x) \end{aligned}$$

observemos que $\varphi + \psi$ é um endomorfismo de G. De fato, dados $x, y \in G$ temos

$$\begin{aligned} (\varphi + \psi)(x * y) &= \varphi(x * y) * \psi(x * y) \\ &= \varphi(x) * \varphi(y) * \psi(x) * \psi(y) \\ &= \varphi(x) * \psi(x) * \varphi(y) * \psi(y) \\ &= (\varphi + \psi)(x) * (\varphi + \psi)(y) \end{aligned}$$

e portanto $(\varphi + \psi) \in End(G)$. Definamos também $\varphi \cdot \psi = \varphi \circ \psi$. Conforme visto no Exemplo 15, temos $\varphi \circ \psi \in End(G)$. Ademais, temos que $End(G)$, munido dessas operações, é um anel com unidade, a saber o endomorfismo identidade, que denotaremos por Id_G. Como a multiplicação do anel $End(G)$ é a composição de funções, temos ainda que $\psi \in U(End(G))$ se, e somente se, ψ é um endomorfismo inversível de G, ou seja, ψ é um automorfismo de G. Logo, $U(End(G)) = Aut\ G$, o grupo dos automorfismos de G.

Estudemos agora o caso particular em que G é o grupo cíclico de ordem n, o qual denotaremos por C_n.

Inicialmente, observemos que a aplicação

$$\begin{aligned} \psi : C_n &\longrightarrow C_n \\ x &\longmapsto \psi(x) = x^m \end{aligned}$$

é um endomorfismo de C_n para todo $m \in \mathbb{Z}$, conforme pode ser visto no Exemplo 14. Ademais, mostraremos agora que todo endomorfismo de C_n é desta forma, ou seja, se $\psi \in End(C_n)$, então existe $m \in \mathbb{Z}$ tal que $\psi(x) = x^m$, para todo $x \in C_n$.

Sabemos que C_n é um grupo cíclico, digamos $C_n =< a >$, e tomando $\psi \in End(G)$ temos $\psi(a) = a^m$ para algum $m \in \mathbb{Z}$, uma vez que $\psi(a) \in C_n$. Daí, dado $x \in C_n$, temos $x = a^k$ e portanto

$$\psi(x) = \psi(a^k) = (\psi(a))^k = (a^m)^k = a^{mk} = a^{k^m} = x^m$$

Logo, $\psi(x) = x^m$ para todo $x \in C_n$. Assim, temos $End(C_n) = \{\psi_m \ / \ m \in \mathbb{Z}\}$, onde ψ_m é o endomorfismo de C_n dado por $\psi_m(x) = x^m$ para todo $x \in C_n$.

Consideremos agora a aplicação

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow End(C_n) \\ m &\longmapsto f(m) = \psi_m \end{aligned}$$

temos que f é um homomorfismo de anéis. De fato, dados $n, m \in \mathbb{Z}$ e $x \in C_n$ temos

$$\psi_{n+m}(x) = x^{n+m} = x^n x^m = \psi_n(x)\psi_m(x) = (\psi_n + \psi_m)(x)$$

e

$$\psi_{nm}(x) = x^{nm} = x^{mn} = (x^m)^n = \psi_n(x^m) = \psi_n(\psi_m(x)) = (\psi_n \circ \psi_m)(x)$$

e assim temos $f(n+m) = f(n) + f(m)$ e $f(nm) = f(n)f(m)$. Logo, f é um homomorfismo de anéis como afirmamos anteriormente. Ademais, como $End(C_n) = \{\psi_m \ / \ m \in \mathbb{Z}\}$ temos que f é sobrejetivo.

Observemos agora que $Kerf = \{m \in \mathbb{Z} \ / \ \psi_m(x) = e, \ \forall \ x \in C_n\}$. Assim, se $m \in Kerf$, particularmente teremos $\psi_m(a) = a^m = e$ e portanto (vide Observação 3, página 16), temos que $n = o(a)$ divide m, ou seja, $m = nk$, com $k \in \mathbb{Z}$. Ademais, $m = nk$ satisfaz $x^m = e$, para todo $x \in C_n$, pois $n = |C_n|$. Portanto, $Kerf = n\mathbb{Z}$. Daí, pelo Teorema Fundamental dos Homomorfismos (vide Teorema 8, página 33), teremos $\mathbb{Z}_n = \dfrac{\mathbb{Z}}{n\mathbb{Z}} \simeq End(C_n)$, donde decorre $U(End(C_n)) \simeq U(\mathbb{Z}_n)$ e assim, combinando este resultado com os da subseção 2.2.1, temos uma descrição precisa da estrutura de $U(End(C_n))$.

2.2.3 Grupo Multiplicativo Cíclico Infinito

Sendo K um corpo, recordemos que $K[x]$ é o anel dos polinômios na indeterminada x com coeficientes em K. Conforme comentamos na Observação

15 (veja página 36), $K[x]$ é um DFU. Assim sendo, consideremos seu corpo de frações, o qual iremos denotar por $K(x)$.

Nesta seção iremos estudar a estrutura do grupo multiplicativo de um subanel de $K(x)$, no caso particular onde K é um corpo de 2 elementos.

Consideremos então $K = \{0, 1\}$ um corpo de dois elementos. Definamos

$$A = \left\{ \frac{f(x)}{x^n} \ / f(x) \in K[x] \text{ e } n \in \mathbb{Z}, n \geq 0 \right\}.$$

e observemos que A é um subanel de $K(x)$. De fato, dados $\frac{f(x)}{x^n}, \frac{g(x)}{x^m} \in A$ temos

$$\frac{f(x)}{x^n} - \frac{g(x)}{x^m} = \frac{x^m f(x) - x^n g(x)}{x^{nm}} \in A$$

e

$$\frac{f(x)}{x^n}\frac{g(x)}{x^m} = \frac{f(x)g(x)}{x^{nm}} \in A$$

Daí, A é subanel de $K(x)$ como afirmamos. Ademais, notemos que $1 = \frac{x^n}{x^n} \in A$ e como $K(x)$ é comutativo segue que A é um anel comutativo com unidade.

Assim, como A é um anel com unidade, faz sentido estudarmos $U(A)$. Observemos que dado $a = \frac{f(x)}{x^n} \in U(A)$, devemos ter $a^{-1} = \frac{g(x)}{x^m}$, e daí $1 = aa^{-1} = \frac{f(x)g(x)}{x^{nm}}$. Portanto $f(x)g(x) = x^{nm}$. Assim, como $K[x]$ é um DFU e x é um elemento irredutível, devemos ter $f(x) = x^{k_1}$ e portanto $a = x^{k_1 - n}$, ou seja, $a \in < x >= \{x^k \ / \ k \in \mathbb{Z}\}$. Logo, $U(A) \subseteq < x >$. Por outro lado, claramente $< x > \subseteq U(A)$ e temos então $U(A) = < x >$. Observemos também que como não existe $n \in \mathbb{N}$ tal que $x^n = 1$, temos $o(x) = | < x > | = \infty$ em $U(A)$, e portanto $U(A)$ é um grupo cíclico e infinito.

Para finalizarmos esta Seção, iremos mostrar que $U(A)$ é isomorfo a $(\mathbb{Z}, +)$ e tendo mostrado isso, fica comprovado que $U(A)$ possui as mesmas propriedades algébricas de $(\mathbb{Z}, +)$, propriedades estas que são largamente abordadas na literatura clássica.

Para mostrarmos esse isomorfismo, consideremos a seguinte aplicação

$$\begin{aligned} \psi : \mathbb{Z} &\longrightarrow U(A) \\ m &\longmapsto \psi(m) = x^m \end{aligned}$$

e observemos que ψ é um homomorfismo de grupos. De fato, dados $n, m \in \mathbb{Z}$ temos

$$\psi(n + m) = x^{n+m} = x^n x^m = \psi(n)\psi(m)$$

Observemos também que $Ker\ \psi = \{m \in \mathbb{Z} \ / \ x^m = 1\}$ e, como $o(x) = \infty$, temos $Ker\ \psi = \{0\}$ e portanto ψ é um homomorfismo injetivo de grupos.

Ademais, como $U(A) =< x >$, segue que ψ é sobrejetivo e temos o isomorfismo desejado.

Como último comentário desta seção, gostaríamos de informar que no Capítulo 3 voltaremos a abordar $K(x)$ e lá apresentaremos uma descrição da estrutura de seu grupo multiplicativo.

2.2.4 Anel dos Quatérnios

Nesta seção iremos apresentar e estudar o anel dos quatérnios. Existem várias maneiras de se interpretar os quatérnios, e nesta seção iremos interpretá-los como um subanel do anel de matrizes $M_4(\mathbb{R})$. Para os leitores interessados, uma outra abordagem pode ser encontrada em [6].

Inicialmente, consideremos

$$I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad , \quad i = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$j = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \quad \text{e} \quad k = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}.$$

Consideremos também $R = \{aI + bi + cj + dk \ / \ a, b, c, d \in \mathbb{R}\}$. Notemos que, como $i^2 = j^2 = k^2 = -I$ e $ij = -ji = k, jk = -kj = i, ki = -ik = j$, temos R multiplicativamente fechado. De fato, dados $A, B \in R$, digamos $A = a_1I + b_1i + c_1j + d_1k$ e $B = a_2I + b_2i + c_2j + d_2k$, temos

$$\begin{aligned} AB = {} & (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)I + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)i + \\ & + (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)j + (a_1c_2 + b_1c_2 - c_1b_2 + d_1a_2)k \in R \end{aligned}$$

Observemos que dada $A \in R$, temos $A = aI + bi + cj + dk$, com $a, b, c, d \in \mathbb{R}$. Assim, observando que $A^t = aI - bi - cj - dk$ (onde A^t denota a matriz transposta de A), podemos concluir que $A^tA = AA^t = (a^2 + b^2 + c^2 + d^2)I$. Ademais, se $A \neq 0_4$, onde 0_4 denota a matriz nula 4×4, temos que $(a^2 + b^2 + c^2 + d^2) \neq 0$ e

$$A\left(\frac{1}{a^2 + b^2 + c^2 + d^2}A^t\right) = A^t\left(\frac{1}{a^2 + b^2 + c^2 + d^2}A\right) = I,$$

ou seja, A é inversível em R (vide Exemplo 20, página 27). Portanto, R é um anel com divisão. Entretanto, R não é um corpo, uma vez que $ij = k \neq -k = ji$.

Consideremos agora o conjunto

$$S = \{aI + bi + cj + dk \ / \ a, b, c, d \in \mathbb{Z}\} \subset R \ .$$

Usando raciocínio análogo, ao usado para mostrar o fechamento multiplicativo de R, mostra-se que S é um subanel de R. Observe que $I \in S$ e assim S é um anel com unidade.

Nos dediquemos então, ao estudo dos elementos inversíveis de S. Primeiramente, é imediato que $\{I, -I, i, -i, j, -j, k, -k\} \subseteq U(S)$. Notemos agora que sendo $A \in U(S)$, temos

$$A = aI + bi + cj + dk = \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix}$$

e consequentemente $detA = (a^2 + b^2 + c^2 + d^2)^2 \geq 0$ e $detA \in \mathbb{Z}$. Ademais, existe $B \in S$ tal que $AB = I$ e assim $(detA)(detB) = detI = 1$. Como $detB$ é também um inteiro, devemos ter $detA = a^2 + b^2 + c^2 + d^2 = 1$ e como $a, b, c, d \in \mathbb{Z}$, isto ocorre apenas quando um destes números for ± 1 e os demais iguais a 0. Portanto, $U(S) = \{I, -I, i, -i, j, -j, k, -k\}$.

Para finalizarmos esta seção, gostaríamos de chamar atenção para o fato de que $U(S)$ é um grupo de ordem 8, não abeliano e que possui um único elemento de ordem 2, a saber $-I$. Portanto, de acordo com a classificação dos grupos de ordem 8, apresentada na Tabela 1.1, decorre que $U(S) \simeq Q_8$ (veja o Exemplo 4, página 17).

2.2.5 Grupo multiplicativo $U(\mathbb{Z}[\sqrt{p}])$

Façamos agora um estudo semelhante ao feito na seção 2.2.1 para o grupo multiplicativo do anel $\mathbb{Z}[\sqrt{p}]$. Recordemos que o anel $\mathbb{Z}[\sqrt{p}]$ foi definido no Exemplo 24.

Neste ponto gostaríamos de destacar que, como poderá ser observado no decorrer desta seção, as técnicas que utilizaremos para o estudo de $U(\mathbb{Z}[\sqrt{p}])$ diferem absolutamente das técnicas utilizadas até agora neste trabalho, envolvendo até conceitos básicos de análise na reta, os quais relembraremos agora.

Dizemos que uma sequência $(a_n)_{n\in\mathbb{N}}$ de números reais converge para um número $a \in \mathbb{R}$ se sempre que dado $\epsilon > 0$ existe um $n_0 \in \mathbb{N}$ tal que

$$n \geq n_0 \implies |a_n - a| < \epsilon$$

Um outro conceito que se fará necessário no decorrer desta seção é o conceito de sequências de Cauchy. Dizemos que uma sequência $(a_n)_{n\in\mathbb{N}}$ de números reais é uma sequência de Cauchy se dado $\epsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que

$$n, m \geq n_0 \implies |a_n - a_m| < \epsilon$$

Destacamos aqui que existe um teorema que relaciona sequências convergentes e sequências de cauchy. O enunciado deste teorema segue abaixo.

Teorema 21. *Uma sequência de números reais é convergente, se e somente se, é uma sequência de Cauchy.*

Outro conceito que utilizaremos nesta seção é o de sequências limitadas. Diremos que uma sequência (a_n) é limitada se existe $M \in \mathbb{R}$, com $M \geq 0$, tal que $|a_n| \leq M$, para todo $n \in \mathbb{N}$.

Também se fará necessário nesta seção o conceito de sequências monótonas. Recordemos que uma sequência (a_n) é dita monótona não decrescente (respectivamente não crescente) se vale $a_n \leq a_{n+1}$ (respectivamente $a_n \geq a_{n+1}$) para todo $n \in \mathbb{N}$.

Assim, como no caso de sequências convergentes e sequências de cauchy, existe um teorema, conhecido como Teorema de Weierstrass, que relaciona sequências monótonas limitadas e sequências convergentes.

Teorema 22. (Teorema de Weierstrass) *Toda sequência de números reais monótona e limitada é convergente.*

Relembraremos agora um conceito que será um ponto chave no estudo que será realizado nesta seção, que é o conceito de ponto isolado. Sendo $X \subset \mathbb{R}$ e $x \in X$, dizemos que x é um ponto isolado de X se existe um $\epsilon > 0$ tal que $X \cap (x - \epsilon, x + \epsilon) = \{x\}$. Maiores detalhes sobre esses conceitos e mais propriedades relativas aos mesmos, assim como as demonstrações dos teoremas 21 e 22, poderão ser consultadas em [9].

Mostremos agora que embora à primeira vista estes conceitos e o grupo multiplicativo de $\mathbb{Z}[\sqrt{p}]$ não estejam diretamente relacionados, isso não ocorre em absoluto.

No decorrer desta seção denotaremos $(\mathbb{R}, +)$ simplesmente por $\mathbb{R}$.

Lema 3. *Se H é um subgrupo aditivo, não nulo, de $\mathbb{R}$ tal que 0 é um ponto isolado de H, então H possui um menor elemento positivo.*

Demonstração. Inicialmente, notemos que como 0 é ponto isolado de H existe $\varepsilon_0 \in \mathbb{R}$, com $\varepsilon_0 > 0$, tal que $(-\varepsilon_0, \varepsilon_0) \cap H = \{0\}$.

Denotemos por H^+ o conjunto dos elementos positivos de H e suponhamos, por absurdo, que H^+ não admite menor elemento. Assim, podemos

construir $(x_n)_{n\in\mathbb{N}} \subset H^+$ tal que $(x_n)_{n\in\mathbb{N}}$ seja monótona, decrescente e limitada inferiormente por 0. De fato, basta tomar um elemento $x_1 \in H^+$, e como H^+ não possui um menor elemento, deve existir $x_2 \in H^+$ tal que $x_2 < x_1$. Prosseguindo deste modo construímos $(x_n)_{n\in\mathbb{N}} \subset H^+$ nas condições desejadas.

Notemos que o Teorema 22 nos garante que $(x_n)_{n\in\mathbb{N}}$ é uma sequência convergente, e assim, pelo Teorema 21, temos que $(x_n)_{n\in\mathbb{N}}$ é uma sequência de Cauchy. Logo, existem $m, n \in \mathbb{N}$, com $m > n$, tais que

$$0 < x_n - x_m = |x_n - x_m| < \varepsilon_0$$

Como H é subgrupo de $\mathbb{R}$ e $(x_n) \subset H$, deveríamos ter $x_n - x_m \in H^+ \cap (0, \varepsilon_0)$, o que é um absurdo. Logo, temos o resultado. □

Uma consequência imediata do Lema 3 é o teorema a seguir.

Teorema 23. *Se H é um subgrupo aditivo, não nulo, de $\mathbb{R}$ tal que 0 é um ponto isolado de H, então H é cíclico e infinito.*

Demonstração. Inicialmente, como $\mathbb{R}$ é livre de torção e $H \neq \{0\}$, devemos ter H infinito. Do Lema 3, segue que existe $\alpha \in H^+$ tal que $\alpha \leq x$, para todo $x \in H^+$. Mostremos agora que $< \alpha >= \{n\alpha \ / \ n \in \mathbb{Z}\} = H$. De fato, é imediato que $< \alpha > \subseteq H$, pois $\alpha \in H$. Suponhamos então que $H \not\subseteq < \alpha >$. Como $\alpha \in \mathbb{R}$ e $\alpha > 0$, temos $\mathbb{R} = \bigcup_{n\in\mathbb{Z}} [n\alpha, (n+1)\alpha]$, e assim deveriam existir $\beta \in H$ e $m \in \mathbb{Z}$, tais que $m\alpha < \beta < (m+1)\alpha$. Daí, teríamos

$$0 < (m+1)\alpha - \beta < (m+1)\alpha - m\alpha = \alpha$$

e assim $(m+1)\alpha - \beta \in H^+$, o que seria um absurdo. Logo, $H = < \alpha >$. □

Nos dediquemos agora ao estudo do grupo multiplicativo $U(\mathbb{Z}[\sqrt{p}])$.

Consideremos a seguinte aplicação:

$$\begin{aligned} N : \ \mathbb{Z}[\sqrt{p}] &\longrightarrow \mathbb{Z}_+ \\ a + b\sqrt{p} &\longmapsto N(a + b\sqrt{p}) = |a^2 - pb^2| \end{aligned}$$

e notemos que dados $x = a + b\sqrt{p}$, $y = c + d\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$ temos

$$\begin{aligned} N(xy) &= |(ac + pbd)^2 - p(bc + ad)^2| \\ &= |(a^2c^2 + 2acpbd + p^2b^2d^2) - p(b^2c^2 + 2bcad + a^2d^2)| \\ &= |a^2c^2 + 2acpbd + p^2b^2d^2 - pb^2c^2 - 2pbcad - pa^2d^2)| \\ &= |a^2c^2 + p^2b^2d^2 - pb^2c^2 - pa^2d^2)| \\ &= |(a^2 - pb^2)(c^2 - pd^2)| \\ &= N(x)N(y). \end{aligned}$$

Notemos também que $x \in U(\mathbb{Z}[\sqrt{p}])$ se, e somente se, $N(x) = 1$. De fato, se $x \in U(\mathbb{Z}[\sqrt{p}])$, então $x, x^{-1} \neq 0$ e daí $N(x), N(x^{-1}) \neq 0$. Logo,

$$1 \leq N(x) \leq \ N(x)N(x^{-1}) = N(xx^{-1}) = N(1) = 1$$

e portanto $N(x) = 1$.

Reciprocamente, se $N(x) = 1$ e $x = a + b\sqrt{p}$, temos que $N(x) = |x\overline{x}|$, onde $\overline{x} = a - b\sqrt{p}$, e daí devemos ter $x\overline{x} = 1$ ou $x\overline{x} = -1$. Se $x\overline{x} = 1$, temos que x é inversível; se $x\overline{x} = -1$, temos $x\overline{(-x)} = 1$ e daí x é inversível.

Consideremos agora o conjunto $A = \{\alpha \in U(\mathbb{Z}[\sqrt{p}]) \ / \ \alpha > 0\}$ e observemos que A é um subgrupo de $U(\mathbb{Z}[\sqrt{p}])$. Mostremos que 1 é ponto isolado de A. De fato, sendo $x = a + b\sqrt{p} \in A$ e $x > 1$, então $N(x) = |a^2 - pb^2| = 1$. Daí, $a^2 - pb^2 = 1$ ou $a^2 - pb^2 = -1$:
• Se $a^2 - pb^2 = 1$, então $(a + b\sqrt{p})(a - b\sqrt{p}) = 1$. Daí, $a - b\sqrt{p} = \frac{1}{a+b\sqrt{p}}$ e portanto $0 < a - b\sqrt{p} < 1$ visto que $a + b\sqrt{p} > 1$. Observemos que se $a < 0$, como $b\sqrt{p} < a$, deveríamos ter $b < 0$ e daí $a + b\sqrt{p} < 0$ o que seria uma contradição. Logo, $a > 0$ e portanto $a \geq 1$, e como $b \neq 0$, devemos ter $b > 0$, pois se $b < 0$, teríamos $a - b\sqrt{p} > 1$ e daí $a + b\sqrt{p} < 1$. Assim, $x = a + b\sqrt{p} > 2$.
• Se $a^2 - pb^2 = -1$, então $(a + b\sqrt{p})(a - b\sqrt{p}) = -1$. Daí, $a - b\sqrt{p} = \frac{-1}{a+b\sqrt{p}}$ e portanto $-1 < a - b\sqrt{p} < 0$, uma vez que $a + b\sqrt{p} > 1$. Assim, temos $a < b\sqrt{p}$, e notemos que se $b < 0$ teríamos $a < b\sqrt{p} < 0$, donde $a + b\sqrt{p} < 0$, o que seria um absurdo. Logo, $b > 0$, e daí $b\sqrt{p} > 1$. Portanto $0 < -1 + b\sqrt{p} < a$. Logo, $1 \leq a < b\sqrt{p}$, e consequentemente $x = a + b\sqrt{p} > 2$.

Sendo $x = a + b\sqrt{p} \in A$ e $0 < x < 1$, então $x^{-1} > 1$. Logo, $x^{-1} > 2$ e portanto $x < \frac{1}{2}$. Assim, 1 é ponto isolado de A como afirmado anteriormente.

Observemos agora que a função

$$\begin{aligned} \varphi : A &\longrightarrow \mathbb{R} \\ \alpha &\longmapsto \varphi(\alpha) = \ln \alpha \end{aligned}$$

onde ln denota o logarítmo natural, é um homomorfismo injetivo de grupos. De fato, dados $\alpha, \beta \in A$, temos $\varphi(\alpha\beta) = \ln(\alpha\beta) = \ln(\alpha) + \ln(\beta) = \varphi(\alpha) + \varphi(\beta)$ e $\ln(\alpha) = \ln(\beta)$ se, e somente se, $\alpha = \beta$. Ademais, como 1 é ponto isolado de A, devemos ter $0 = \varphi(1)$ ponto isolado de $H = \varphi(A)$, visto que sendo $\alpha \in A$, então $\alpha < \frac{1}{2}$ ou $\alpha > 2$, e daí $\ln(\alpha) > \ln 2$ ou $\ln(\alpha) < -\ln 2$. Portanto, pelo Teorema 23, temos que $H = \varphi(A)$ é cíclico e infinito. Como φ é injetor, temos $A \simeq \varphi(A) = H$ e daí A é um grupo cíclico infinito.

Assim, de posse dessas informações temos todas as ferramentas necessárias para descrever a estrutura do grupo multiplicativo $U(\mathbb{Z}[\sqrt{p}])$. Para tal,

basta notarmos que a função

$$\begin{aligned} \psi : A \times \{-1,1\} &\longrightarrow U(\mathbb{Z}[\sqrt{p}]) \\ (\alpha, k) &\longmapsto \psi(\alpha, k) = k\alpha \end{aligned}$$

é um isomorfismo de grupos. De fato, dados $(a, k_1), (b, k_2) \in A \times \{-1, 1\}$. temos

$$\begin{aligned} \psi(ab, k_1k_2) &= abk_1k_2 \\ &= ak_1bk_2 \\ &= \psi(a, k_1)\psi(b, k_2) \end{aligned}$$

e observemos que a sobrejetividade de ψ segue do fato que se $\alpha \in U(\mathbb{Z}[\sqrt{p}])$, então $\alpha \in A$ ou $\alpha = -\beta$, com $\beta \in A$. Observemos também que a injetividade decorre de todos os elementos de A serem positivos e $k \in \{-1, 1\}$. Portanto, $U(\mathbb{Z}[\sqrt{p}])$ é isomorfo a um produto direto de um grupo cíclico infinito pelo grupo multiplicativo $\{-1, 1\}$. Logo, $U(\mathbb{Z}[\sqrt{p}]) \simeq \mathbb{Z} \times C_2$.

Um outro fato bastante curioso decorrente desta descrição que acabamos de apresentar, é que o fato de dois anéis terem as mesmas estruturas de grupos aditivos e multiplicativos não nos garante que estes anéis tem a mesma estrutura como anéis, ou seja, não necessariamente os anéis em questão são isomorfos. Para um exemplo onde podemos observar esta situação, basta tomar $p, q \in \mathbb{N}$ dois primos distintos e teremos $(\mathbb{Z}[\sqrt{p}], +) \simeq \mathbb{Z} \times \mathbb{Z} \simeq (\mathbb{Z}[\sqrt{q}], +)$ e $U(\mathbb{Z}[\sqrt{p}]) \simeq U(\mathbb{Z}[\sqrt{q}])$. Contudo mostremos agora que $\mathbb{Z}[\sqrt{p}] \not\simeq \mathbb{Z}[\sqrt{q}]$ como anéis. De fato, suponhamos $\mathbb{Z}[\sqrt{p}] \simeq \mathbb{Z}[\sqrt{q}]$ e $f : \mathbb{Z}[\sqrt{p}] \longrightarrow \mathbb{Z}[\sqrt{q}]$ um isomorfismo. Observemos que $f(1) = 1$ e daí $f(n) = n$, para todo $n \in \mathbb{Z}$. Assim, $p = f(p) = f(\sqrt{p}^2) = f(\sqrt{p})^2$. Entretanto, $f(\sqrt{p}) \in \mathbb{Z}[\sqrt{q}]$ e em $\mathbb{Z}[\sqrt{q}]$ não existe elemento com essa propriedade, pois caso $(a + b\sqrt{q})^2 = p$ (com $a, b \in \mathbb{Z}$), deveríamos ter $(a^2 + qb^2) + 2ab\sqrt{q} = p$, donde $2ab = 0$ e $a^2 + qb^2 = p$ o que seria um absurdo, pois $a, b \in \mathbb{Z}$. Assim, os anéis $\mathbb{Z}[\sqrt{p}]$ constituem uma família infinita de anéis que possuem as mesmas estruturas de grupos aditivos e multiplicativos mas não são isomorfos.

2.3 Grupos Multiplicativos Abelianos de Ordem Ímpar

Nesta seção iremos estudar e elencar alguns resultados, provenientes da teoria de anéis e da teoria básica de álgebra comutativa, que combinados nos

darão uma condição necessária para que um grupo abeliano finito de ordem ímpar seja grupo multiplicativo de algum anel.

Iniciaremos esse estudo demonstrando um resultado que, em condições específicas, nos garante a associatividade entre soma e interseção de ideais.

Proposição 3. ***(Lei Modular de Dedekind)*** *Se I_1, I_2 e I_3 são ideais de um anel A, com $I_1 \subseteq I_3$, então*

$$(I_1 + I_2) \cap I_3 = I_1 + (I_2 \cap I_3)$$

Demonstração. Seja $x \in (I_1 + I_2) \cap I_3$. Daí $x = h + k$, onde $h \in I_1$, $k \in I_2$, e $h + k \in I_3$. Como $I_1 \subseteq I_3$, temos que $h, -h \in I_3$. Por outro lado, sendo $h + k = x \in I_3$ temos que $k = x - h \in I_3$. Assim, $k \in I_2 \cap I_3$ e portanto $h + k \in I_1 + (I_2 \cap I_3)$. Logo, $(I_1 + I_2) \cap I_3 \subseteq I_1 + (I_2 \cap I_3)$.

Reciprocamente, seja $y \in I_1 + (I_2 \cap I_3)$. Então, $y = h + k$, onde $h \in I_1$, e $k \in I_2 \cap I_3$. Como $I_1 \subseteq I_3$, temos $h, k \in I_3$, donde $y \in I_3$. Logo, $y \in (I_1 + I_2) \cap I_3$ e portanto $I_1 + (I_2 \cap I_3) \subseteq (I_1 + I_2) \cap I_3$. □

Recordemos agora que sendo A um anel comutativo com unidade todo elemento não inversível de A pertence a algum ideal maximal de A (vide Observação 10, página 31).

Neste ponto iremos definir alguns conceitos básicos de álgebra comutativa e a partir dessas definições provaremos diversos resultados que auxiliarão na classificação desejada.

Definição 41. Sendo A um anel comutativo e com unidade, definimos o radical de Jacobson de A, denotado por $J(A)$, como sendo a interseção de todos os ideais maximais de A.

Sendo A um anel comutativo e com unidade, $J(A)$ é um ideal de A. Ademais, podemos caracterizar os elementos de $J(A)$ através do resultado a seguir.

Proposição 4. *Sejam A um anel comutativo com unidade e $a \in A$. São equivalentes:*

i) $a \in J(A)$;

ii) $ax - 1$ é inversível em A, para todo $x \in A$.

Demonstração. *i)* $\implies$ *ii)* Admitindo $a \in J(A)$, suponhamos, por contradição, que $ax - 1 \notin U(A)$, para algum $x \in A$. Daí, como A é um anel comutativo com unidade, temos que $ax - 1 \in M$, para algum M ideal maximal de A. Assim, $ax - 1 = m \in M$.

Como $a \in J(A) \subseteq M$, segue que $a \in M$, donde $ax \in M$ e portanto devemos ter $1 = m - xa \in M$, o que é um absurdo, pois $M \neq A$. Logo, $ax - 1 \in U(A)$, para todo $x \in A$.

ii) $\Longrightarrow$ *i)* Admitindo agora que $ax - 1 \in U(A)$, para todo $x \in A$, suponhamos, por contradição, que $a \notin J(A)$. Então, deve existir M ideal maximal de A tal que $a \notin M$. Como $a \notin M$, devemos ter $M \subsetneq M + < a >$. Entretanto, M é um ideal maximal de A, logo $M + < a >= A$. Assim, devem existir $m \in M$ e $x \in A$ tais que $m + ax = 1$. Daí, $ax - 1 = -m \in M$, o que é um absurdo, visto que $ax - 1 \in U(A)$ e $M \neq A$. Portanto, $a \in J(A)$. □

De posse dessas equivalências podemos assegurar a distributividade do radical de Jacobson em relação ao produto direto. Enunciaremos este resultado com maior rigor no teorema a seguir.

Teorema 24. *Sejam A e A_1 anéis comutativos com unidade. Então, devemos ter $J(A \times A_1) = J(A) \times J(A_1)$.*

Demonstração. Sejam $(a, a_1) \in J(A \times A_1)$, 1 a unidade de A_1 e 1_A a unidade de A. Para todo $(x, y) \in A \times A_1$, pela Proposição 4 temos

$$(ax - 1_A, a_1 y - 1) = (a, a_1)(x, y) - (1_A, 1) \in U(A \times A_1)$$

Daí, $ax - 1_a \in U(A)$ e $a_1 y - 1 \in U(A_1)$. Consequentemente, $a \in J(A)$ e $a_1 \in J(A_1)$. Portanto, $J(A \times A_1) \subseteq J(A) \times J(A_1)$. A inclusão contrária pode ser demonstrada analogamente, e o resultado segue. □

Dando sequência ao estudo do Radical de Jacobson de um anel, demonstraremos agora algumas propriedades decorrentes do caso em que um anel finito A é tal que $J(A) = \{0\}$.

Porém, antes de apresentarmos essas propriedades, estabeleçamos o conceito de complemento de um ideal.

Definição 42. Sejam A um anel comutativo com unidade e I um ideal de A. Definimos um complemento para I em A como sendo um ideal J de A tal que $I \cap J = \{0\}$ e $I + J = A$.

Teorema 25. *Sendo A um anel comutativo com unidade finito, são equivalentes:*

i) $J(A) = \{0\}$;

ii) Todo ideal de A possui complemento.

Demonstração. i) $\Longrightarrow$ *ii)* Seja J um ideal arbitrário de A e considere o conjunto

$$I_J = \{I \text{ ideal de } A \ / \ I + J = A\}$$

Claramente, I_J é não-vazio visto que $A \in I_J$. Como A é um anel finito, tomemos I_0 minimal em I_J e mostremos que $I_0 \cap J = \{0\}$. Para tal, suponhamos por contradição, que $I_0 \cap J \neq \{0\}$. Então existe algum ideal maximal M de

A tal que $I_0 \cap J \not\subseteq M$, uma vez que $J(A) = \{0\}$. Então, $M \subsetneq M + (I_0 \cap J)$ e daí, como M é maximal, devemos ter $M + (I_0 \cap J) = A$.

Assim, $I_0 = ((I_0 \cap J) + M) \cap I_0$ e portanto, pela Proposição 3, devemos ter $I_0 = (I_0 \cap J) + (M \cap I_0)$, e daí $J + I_0 = J + (M \cap I_0)$. Como $I_0 \in I_J$, devemos ter $A = J + (M \cap I_0)$. Logo, $M \cap I_0 \in I_J$. Mas, I_0 é minimal em I_J, o que acarreta $M \cap I_0 = I_0$ e assim $I_0 \subseteq M$, o que é um absurdo, uma vez que $I_0 \cap J \not\subseteq M$. Logo, $I_0 \cap J = \{0\}$ e portanto I_0 é um complemento para J em A.

ii) $\Rightarrow$ *i)* Suponhamos, por contradição, que $J(A) \neq \{0\}$. Por hipótese, deve existir J ideal de A tal que J é um complemento para $J(A)$ em A, ou seja, $J(A) + J = A$ e $J(A) \cap J = \{0\}$. Como J é um ideal próprio de A, deve existir M ideal maximal de A, com $J \subseteq M$. Daí, como $J(A) \subseteq M$, devemos ter $A = J(A) + J \subseteq M$, o que é um absurdo, visto que M é um ideal maximal de A. Logo, $J(A) = \{0\}$. □

Mostremos agora que a propriedade de todo ideal admitir complemento em um anel comutativo com unidade A, que no caso particular de A finito é equivalente a $J(A) = \{0\}$, tem fortes implicações na estrutura de A.

Teorema 26. *Seja A um anel comutativo com unidade. São equivalentes:*

i)$A \simeq A_1 \times A_2$, com A_1 e A_2 anéis não nulos;

ii) Existem I e J ideais não nulos de A tais que $I \cap J = \{0\}$ e $I + J = A$.

Demonstração. i) $\Longrightarrow$ *ii)* Seja $\varphi : A_1 \times A_2 \to A$ um isomorfismo e consideremos $I = \varphi(A_1 \times \{0\})$ e $J = \varphi(\{0\} \times A_2)$. Como $A_1 \times \{0\}$ e $\{0\} \times A_2$ são ideais de $A_1 \times A_2$ e φ é um isomorfismo, segue que I e J são ideais de A (vide Observação 12, página 32). Ademais, temos claramente que $I + J = A$ e $I \cap J = \{0\}$.

ii) $\Rightarrow$ *i)* Como os ideais I e J são não nulos, nas condições dadas devemos ter I e J ideais próprios e assim os anéis quociente $A_1 = \frac{A}{I}$ e $A_2 = \frac{A}{J}$ também são não nulos.

Consideremos a aplicação $\varphi : A \to A_1 \times A_2$ dada por $\varphi(a) = (\overline{a}, \overline{\overline{a}})$, onde $\overline{a} = a + I$ e $\overline{\overline{a}} = a + J$. Das propriedades de anéis quocientes segue que φ é um homomorfismo de anéis. Como

$$Ker\varphi = \{a \in A \ / \ \varphi(a) = (\overline{0}, \overline{\overline{0}})\} = I \cap J = \{0\}$$

segue que φ é injetiva. Ademais, temos que φ é sobrejetiva. De fato, como $I + J = A$, existem $a \in I$ e $b \in J$ tais que $1 = a + b$. Assim, dado

$(\overline{x}, \overline{\overline{y}}) \in A_1 \times A_2$ tomando $k = xb + ya \in A$ temos

$$\begin{aligned}
\varphi(k) &= (\overline{xb + ya}, \overline{\overline{xb + ya}}) \\
&= (\overline{xb}, \overline{\overline{ya}}) \\
&= (\overline{x(1-a)}, \overline{\overline{y(1-b)}}) \\
&= (\overline{x - xa}, \overline{\overline{y - yb}}) \\
&= (\overline{x} - \overline{xa}, \overline{\overline{y}} - \overline{\overline{yb}}) \\
&= (\overline{x}, \overline{\overline{y}})
\end{aligned}$$

Logo, $A \simeq A_1 \times A_2$. □

Assim, usando esse teorema podemos caracterizar anéis finitos com unidade cujo radical de Jacobson é nulo. Temos então o seguinte resultado.

Teorema 27. *Seja A um anel comutativo com unidade finito tal que $J(A) = \{0\}$. Então, $A \simeq K_1 \times K_2 \times ... \times K_t$, onde K_i é um corpo para cada $i = 1, 2, ..., t$.*

Demonstração. Demonstraremos esse teorema por indução em $|A|$. Se $|A| = 2$, então A é um corpo e temos o resultado. Suponhamos então $n > 2$ e, por hipótese de indução, que o resultado vale para todo anel de ordem $m < n = |A|$.

Sejam $|A| = n$ e $J(A) = \{0\}$. Supondo que A não é um corpo, então pelo Teorema 6, podemos tomar I ideal de A, com $\{0\} \neq I \neq A$. Assim, do Teorema 25, segue que I possui um complemento em A. Logo, pelo Teorema 26, temos que $A \simeq A_1 \times A_2$, onde A_1 e A_2 são anéis não nulos. Assim, devemos ter $|A_1|, |A_2| < |A|$, $J(A_1) \times J(A_2) = J(A_1 \times A_2)$ e $J(A_1 \times A_2)$ nulo. Daí, por hipótese de indução, temos

$$A_1 \simeq K_{11} \times ... \times K_{1r} \text{ e } A_2 \simeq K_{21} \times ... \times K_{2s}$$

onde cada K_{1i} e cada K_{2j} é um corpo, para $i = 1, 2, ..., r$ e $j = 1, 2, ..., s$. Logo, $A \simeq K_{11} \times ... \times K_{1r} \times K_{21} \times ... \times K_{2s}$ e temos o resultado. □

Introduziremos agora um outro conceito que irá nos auxiliar a refinar a caracterização dada pelo Teorema 27, no caso particular em que a ordem do anel A é ímpar.

Definição 43. Sendo A um anel comutativo com unidade, definimos o nilradical de A, denotado por $N(A)$, como sendo o conjunto de todos os elementos nilpotentes de A.

Notemos que $N(A)$ é um ideal de A. De fato, tomando arbitrariamente $x, y \in N(A)$ e $a \in A$, temos que existem $n, m \in \mathbb{N}$ tais que $x^n = y^m = 0$, e daí $(xa)^n = x^n a^n = 0$, ou seja, $xa \in N(A)$. Ademais, do binômio de Newton, temos que $(x+y)^{n+m} = \sum_{j=0}^{n+m} \binom{n+m}{j} x^{n+m-j} y^j = 0$, visto que cada parcela do somatório é da forma $c_d x^r y^s$, onde $c_d \in \mathbb{N}$ e $r \geq n$ ou $s \geq m$, ou seja, $x^r = 0$ ou $y^s = 0$. Daí, $x + y \in N(A)$ e portanto $N(A)$ é um ideal de A.

Um modo de caracterizar $N(A)$ é dado pela proposição a seguir, cuja demonstração pode ser encontrada em [1].

Proposição 5. *Seja A um anel comutativo com unidade. Então, $N(A)$ é a interseção dos ideais primos de A.*

Recordemos que sendo A um anel comutativo com unidade finito, temos que os conceitos de ideais maximais e ideais primos são equivalentes, isto é, I é um ideal maximal de A se, e somente se, I é um ideal primo de A. Decorre daí que se A é um anel finito comutativo com unidade, então $N(A) = J(A)$, uma vez que $J(A)$ é a interseção de todos os ideais maximais de A, que neste caso coincidem com todos os ideais primos de A.

Consideremos agora A um anel com unidade tal que $U(A)$ seja abeliano, finito e de ordem ímpar, digamos $U(A) = \{x_1, x_2, ..., x_k\}$ e tomemos R como sendo o subgrupo aditivo gerado por $U(A)$, ou seja,

$$R = \{n_1 x_1 + n_2 x_2 + ... + n_k x_k \ / \ n_i \in \mathbb{Z}\}.$$

Claramente, R é um subanel de A (pois $U(A)$ é multiplicativamente fechado) e, como $U(A)$ é abeliano, temos que R é comutativo. Além disso, notemos que $1_A \in R$ e portanto R é um anel comutativo com unidade.

Ademais, observemos que como $-1 \in U(A)$, se $-1 \neq 1$, deveríamos ter $o(-1) = 2$ em $U(A)$ e daí $|U(A)|$ seria divisível por 2, o que seria absurdo. Então, $-1 = 1$ e portanto $charA = charR = 2$. Assim, $nx = x$ ou $nx = 0$, para todo $n \in \mathbb{Z}$ e $x \in R$. Logo, R é um anel finito, e como $1_R = 1_A$, dado $x \in U(R)$ devemos ter $x \in U(A)$, ou seja, $U(R) \subseteq U(A)$. Por outro lado, é fácil ver que $U(A) \subseteq U(R)$. Portanto, $U(R) = U(A)$.

Recordemos que se G é um grupo abeliano finito e $mdc(|G|, n) = 1$, então a função $f : G \longrightarrow G$ dada por $f(x) = x^n$ é uma bijeção (vide Exemplo 14, página 23). Então, como $U(A)$ é um grupo abeliano finito e $|U(A)|$ é ímpar, a aplicação

$$\begin{aligned} f : U(A) &\longrightarrow U(A) \\ x &\longmapsto f(x) = x^2 \end{aligned}$$

é uma bijeção. Assim, considerando a aplicação

$$\begin{aligned} \psi : R &\longrightarrow R \\ z &\longmapsto \psi(z) = z^2 \end{aligned}$$

temos que dado $y \in R$, devemos ter $y = z_1 + ... + z_n$, onde $z_i \in U(A)$. Como a função f é uma bijeção, existem $x_i, ..., x_n \in U(A)$ tais que ${x_i}^2 = z_i$. Portanto, uma vez que $charR = 2$, devemos ter

$$\psi(x_1 + ... + x_n) = (x_1 + ... + x_n)^2 = {x_1}^2 + ... + {x_1}^2 = z_1 + ... + z_n = y$$

Logo, ψ é sobrejetiva, e como R é finito, segue que ψ é uma bijeção.

Suponhamos agora $x \in N(R)$. Daí, existe $k \in \mathbb{N}$ tal que $x^k = 0$. Assim, tomando $m \in \mathbb{N}$ tal que $2^m > k$, devemos ter $\psi^m(x) = x^{2^m} = 0$. Como ψ é uma bijeção, devemos ter ψ^m também uma bijeção. Logo, de $\psi^m(x) = x^{2^m} = 0$, segue que $x = 0$ e portanto $N(R) = 0$.

Ademais, uma vez que R é finito, devemos ter $J(R) = N(R) = \{0\}$ e assim, pelo Teorema 27, temos $R \simeq K_1 \times ... \times K_n$, onde cada K_i é um corpo finito. Como $charR = 2$, devemos ter $charK_i = 2$ e daí $|K_i| = 2^{m_i}$ para todo $i = 1, 2, ..., n$ (vide Teorema 11, página 36). Portanto, $U(R) \simeq {K_1}^* \times ... \times {K_n}^*$ e $|{K_i}^*| = 2^{m_i} - 1$, onde ${K_i}^* = K_i - \{0\} = U(K_i)$, para todo $i = 1, 2, ..., n$.

Logo, temos o seguinte teorema.

Teorema 28. *Seja R um anel tal que $U(R)$ é abeliano, finito e de ordem ímpar. Então, $U(R) \simeq {K_1}^* \times ... \times {K_n}^*$, onde K_i é um corpo e $|{K_i}^*| = 2^{m_i} - 1$, para todo $i = 1, 2, ..., n$.*

Um corolário que segue imediatamente do Teorema 28, é o resultado a seguir.

Corolário 2. *Seja R um anel com unidade tal que $U(R)$ é finito, com $|U(R)| = p$ onde p é um primo ímpar. Então, $|U(R)| = 2^r - 1$ para algum $r \in \mathbb{N}$.*

Demonstração. Como $U(R)$ é finito de ordem prima, temos $U(R)$ cíclico e portanto abeliano. Assim, pelo Teorema 28, temos que $U(R) \simeq {K_1}^* \times ... \times {K_n}^*$, onde K_i é um corpo e $|{K_i}^*| = 2^{m_i} - 1$, para todo $i = 1, 2, ..., n$. Logo,

$$p = |U(R)| = |{K_1}^*||{K_2}^*|...|{K_n}^*| = (2^{m_1} - 1)(2^{m_2} - 1)...(2^{m_n} - 1).$$

Como p é um número primo ímpar, isto ocorre apenas quando $i = 1$, ou seja, quando $p = |U(R)| = 2^r - 1$. □

Destacamos aqui que, no Teorema 28 a hipótese de $U(R)$ ser abeliano, pode ser retirada. A demonstração da versão mais geral do Teorema 28 pode ser encontrada em [2].

2.4 Grupos Multiplicativos de Ordem Menor ou Igual a 11

Para finalizarmos este capítulo, utilizando a classificação dos grupos de ordem menor ou igual a 11, encontrada na Tabela 1.1, faremos uma outra classificação desses grupos no sentido de determinar quais deles são grupos multiplicativos de algum anel.

Entretanto, antes de nos dedicarmos a esse estudo fixemos algumas notações que serão adotadas no decorrer desta seção: C_n irá sempre denotar o grupo cíclico de ordem n, assim como K_n denotará o corpo de ordem n (quando existir). Ademais, nesta seção faremos uso do fato de que o grupo multiplicativo de um corpo finito é cíclico (este resultado será provado na Seção 3.2).

•Grupos de Ordem 1

Sabemos que, a menos de isomorfismo, existe apenas um grupo de ordem 1. Assim, dado G um grupo de ordem 1, observemos que $U(\mathbb{Z}_2) = \{\overline{1}\}$, e dai $G \simeq U(\mathbb{Z}_2)$

•Grupos de Ordem 2

Conforme pode ser visto na Tabela 1.1, existe apenas um grupo de ordem 2 a menos de isomorfismo, a saber C_2

Observemos agora que $U(\mathbb{Z}_3) = \{\overline{1}, \overline{2}\}$ e portanto, sendo G um grupo de ordem 2, temos $G \simeq U(\mathbb{Z}_3)$.

•Grupos de Ordem 3

Conforme pode ser visto na Tabela 1.1, existe apenas um grupo de ordem 3 a menos de isomorfismo, a saber C_3

Consideremos agora o corpo K_4, observando que de fato existe um corpo de 4 elementos, uma vez que $4 = 2^2$ (vide Teorema 11, página 36). Assim, como K_4 é um corpo e $|K_4| = 4$, devemos ter $|U(K_4)| = 3$. Logo, sendo G um grupo de ordem 3, temos $G \simeq U(K_4)$.

•Grupos de Ordem 4

De acordo com a classificação apresentada na Tabela 1.1, a menos de isomorfismo, existem apenas dois grupos de ordem 4, a saber, C_4 e $C_2 \times C_2$.

Observemos agora que $U(\mathbb{Z}_5) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\} =< \overline{2} >$, ou seja, $U(\mathbb{Z}_5) \simeq C_4$. Observemos também que $U(\mathbb{Z}_3 \times \mathbb{Z}_3) = U(\mathbb{Z}_3) \times U(\mathbb{Z}_3) \simeq C_2 \times C_2$ (vide Exemplo 21, página 27). Logo, sendo G um grupo de ordem 4, devemos ter $G \simeq U(\mathbb{Z}_5)$ ou $G \simeq U(\mathbb{Z}_3 \times \mathbb{Z}_3)$.

•Grupos de Ordem 5

Conforme pode ser visto na Tabela 1.1, existe apenas um grupo de ordem 5 a menos de isomorfismo, a saber, C_5. Assim, supondo R um anel tal que $U(R) = C_5$, pelo Corolário 2 deveríamos ter $5 = |C_5| = 2^m - 1$, com $m \in \mathbb{N}$, o que seria um absurdo. Logo, C_5 não é grupo multiplicativo de nenhum anel.

•Grupos de Ordem 6

Recordemos que, conforme foi apresentado na Tabela 1.1, a menos de isomorfismo, existem apenas dois grupos de ordem 6, a saber, C_6 e S_3. Observemos que $C_6 \simeq U(K_7)$, pois $U(K_7)$ é cíclico de ordem 6.

Consideremos agora $F = M_2(K)$, onde $K = K_2$. Como visto no Exemplo 20, temos $U(F) = \{A \in F \ / \ det(A) = 1\}$, ou seja,

$$U(F) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

Logo, $|U(F)| = 6$ e, como $U(F)$ é não abeliano, devemos ter $U(F) \simeq S_3$.

•Grupos de Ordem 7

Como podemos ver na Tabela 1.1, C_7 é o único grupo de ordem 7, a menos de isomorfismo. Assim, ao tomarmos K_8, temos $U(K_8)$ cíclico e $|U(K_8)| = 7$, e portanto $U(K_8) \simeq C_7$.

É importante destacar que, como $8 = 2^3$ pelo Teorema 11, existe de fato tomar K_8.

•Grupos de Ordem 8

Recordemos que (vide Tabela 1.1, página 24), a menos de isomorfismo, os grupos de ordem 8 são:

$$C_8, \quad C_4 \times C_2, \quad C_2 \times C_2 \times C_2, \quad D_4 \quad \text{e} \quad Q_8$$

onde D_4 e Q_8 são os Exemplos 11 e 4 respectivamente, comentados no Capítulo 1.

Como $9 = 3^2$ (vide Teorema 11, página 36) podemos tomar K_9, e daí $U(K_9) = C_8$. Considerando agora o anel $\mathbb{Z}_5 \times \mathbb{Z}_3$, temos (ver Exemplo 21, página 27)

$$U(\mathbb{Z}_5 \times \mathbb{Z}_3) = U(\mathbb{Z}_5) \times U(\mathbb{Z}_3) \simeq C_4 \times C_2 \ .$$

Consideremos também o anel $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ e observemos que (ver Exemplo 21, página 27)

$$U(\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3) = U(\mathbb{Z}_3) \times U(\mathbb{Z}_3) \times U(\mathbb{Z}_3) \simeq C_2 \times C_2 \times C_2 \ .$$

Assim, todos os grupos abelianos de ordem 8 são grupos multiplicativos de anéis.

Passemos agora a estudar os grupos não-abelianos de ordem 8.

Daremos início a esse estudo com o grupo D_4. Iniciaremos considerando $C_4 =< a >= \{e_1, a, a^2, a^3\}$, $C_2 =< b >= \{e_2, b\}$ e $R = End(C_4 \times C_2)$ o anel dos endomorfismos de $C_4 \times C_2$, cujas as operações foram comentadas na Seção 2.2.2. Recordemos que, conforme mostramos na Seção 2.2.2, temos $U(R) = Aut(C_4 \times C_2)$.

Observemos agora que $C_4 \times C_2 =< (a, e_2), (e_1, b) >$ e que $o(a, e_2) = 4$ e $o(e_1, b) = 2$. Assim, como isomorfismos preservam ordem de elementos, devemos ter $o(f(a, e_2)) = 4$ e $o(f(e_1, b)) = 2$, para todo $f \in Aut(C_4 \times C_2)$. Logo, temos, a principio, 4 possibilidades para $f(a, e_2)$ e 3 possibilidades para $f(e_1, b)$ e portanto $|U(R)| \leq 12$, uma vez que se $g \in Aut(C_4 \times C_2)$ é tal que $g(a, e_2) = f(a, e_2)$ e $g(e_1, b) = f(e_1, b)$, então $g = f$.

Tomemos agora $\varphi : (C_4 \times C_2) \longrightarrow (C_4 \times C_2)$, dada por $\varphi(a^m, b^n) = (a^{2n-m}, b^{n+m})$. Mostremos agora que $\varphi \in Aut\ (C_4 \times C_2)$. De fato, dados $(a^m, b^n), (a^r, b^s) \in (C_4 \times C_2)$, temos

$$\begin{aligned}
\varphi(a^m a^r, b^n b^s) &= \varphi(a^{m+r}, b^{n+s}) \\
&= (a^{2(n+s)-(m+r)}, b^{m+r+n+s}) \\
&= (a^{(2n-m)+(2s-r)}, b^{(m+n)+(r+s)}) \\
&= (a^{2n-m} a^{2s-r}, b^{m+n} b^{r+s}) \\
&= (a^{2n-m}, b^{m+n})(a^{2s-r}, b^{r+s}) \\
&= \varphi(a^n, b^m)\varphi(a^r, b^s).
\end{aligned}$$

Logo, $\varphi \in End\ (C_4 \times C_2)$. Ademais,

$$Ker\ \varphi = \{(a^n, b^m) \in C_4 \times C_2 \ / \ (a^{2n-m}, b^{n+m}) = (e_1, e_2)\}.$$

Assim, se $(a^m, b^n) \in Ker\ \varphi$, então $(a^{2n-m}, b^{n+m}) = (e_1, e_2)$ e portanto $2n - m = 4r$ e $n + m = 2s$, com $r, s \in \mathbb{Z}$. Daí, $m = 2(n - 2r)$, ou seja,

m é par, e como $n+m=2s$, temos que n também é par, digamos $n=2t$, e daí $b^n=e_2$. Além disso, sendo $n=2t$, decorre que $m=4(t-r)$ e portanto $a^m=e_1$. Logo, $Ker\varphi=\{(e_1,e_2)\}$ e portanto φ é injetivo. Como $C_4\times C_2$ é finito, segue que φ é uma bijeção e daí $\varphi\in Aut\ C_4\times C_2$.

Observemos que $\varphi(a,e_2)=(a^3,b)$ e $\varphi(e_1,b)=(a^2,b)$, donde

$$\varphi^2(a,e_2)=\varphi(a^3,b)=(a^3,e_2),\quad \text{e}\quad \varphi^2(e_1,b)=\varphi(a^2,b)=(e_1,b)$$

$$\varphi^3(a,e_2)=\varphi(a^3,e_2)=(a,b),\quad \text{e}\quad \varphi^3(e_1,b)=\varphi(e_1,b)=(a^2,b)$$

$$\varphi^4(a,e_2)=\varphi(a,b)=(a,e_2),\quad \text{e}\quad \varphi^4(e_1,b)=\varphi(a^2,b)=(e_1,b)$$

Assim, $\varphi,\varphi^2,\varphi^3\neq Id$ e $\varphi^4=Id$, e portanto $o(\varphi)=4$.

Analogamente, mostra-se que tomando $\sigma: C_4\times C_2\longrightarrow C_4\times C_2$, definida por $\sigma(a^n,b^m)=(a^{n+2m},b^m)$, temos que $\sigma\in Aut(C_4\times C_2)$ e $o(\sigma)=2$. Ademais, $<\sigma>\cap<\varphi>=\{Id\}$, pois $\sigma\notin<\varphi>$, uma vez que o único elemento de ordem 2 de $<\varphi>$ é φ^2 e $\varphi^2\neq\sigma$. Dessa forma, temos que $|<\varphi><\sigma>|=o(\varphi)o(\sigma)=8$.

Notemos agora que

$$\sigma(\varphi(\sigma(a,e_2)))=\sigma(\varphi(a,e_2))=\sigma(a^3,b)=(a,b)=\varphi^{-1}(a,e_2)$$

e também

$$\sigma(\varphi(\sigma(e_1,b)))=\sigma(\varphi(a^2,b))=\sigma(e_1,b)=(a^2,b)=\varphi^{-1}(e_1,b).$$

Portanto, $\sigma\varphi\sigma=\varphi^{-1}$ e assim, $<\varphi,\sigma>=<\varphi><\sigma>$.

Entretanto, $<\varphi,\sigma>$ é um subgrupo de ordem 8 de $Aut(C_4\times C_2)$ e como $|Aut(C_4\times C_2)|\leq 12$, do Teorema de Lagrange (vide Teorema 1, página 18) segue que $|Aut(C_4\times C_2)|=8$, e daí $Aut(C_4\times C_2)=<\varphi,\sigma>$.

Como $o(\varphi)=4$, $o(\sigma)=2$, e $\sigma\varphi\sigma=\varphi^{-1}$ temos, $Aut(C_4\times C_2)\simeq D_4$.

Para finalizarmos o estudo dos grupos multiplicativos de ordem 8, recordemos que na Seção 2.2.4, mostramos que $Q_8\simeq U(S)$, onde S é o subanel $\{aI+bi+cj+dk\ /\ a,b,c,d\in\mathbb{Z}\}$ do anel dos quatérnios reais.

Concluímos assim que todos os grupos de ordem 8 são grupos multiplicativos de anéis.

•Grupos de Ordem 9

Conforme visto na Tabela 1.1, os grupos de ordem 9, a menos de isomorfismo, são C_9 e $C_3\times C_3$.

Observemos que $U(K_4\times K_4)=U(K_4)\times U(K_4)\simeq C_3\times C_3$, conforme visto no Exemplo 21.

Entretanto, se R é um anel tal que $U(R) = C_9$, como C_9 é um grupo abeliano de ordem ímpar, pelo Teorema 28 devemos ter $C_9 \simeq {K_1}^* \times ... \times {K_n}^*$, onde K_i é um corpo e $|{K_i}^*| = 2^{n_i} - 1$, para todo $i = 1, 2, ..., n$. Daí, deveríamos ter $n = 1$ e $|{K_1}^*| = 9$, o que seria um absurdo pois 9 não é da forma $2^m - 1$, ou $n = 2$ e $|{K_1}^*| = 3 = |{K_2}^*|$, donde teríamos $C_9 \simeq C_3 \times C_3$, o que seria um absurdo. Logo, C_9 não é grupo multiplicativo de nenhum anel.

•Grupos de Ordem 10

Conforme apresentamos na Tabela 1.1, os grupos de ordem 10, a menos de isomorfismo, são C_{10} e D_5, onde D_5 denota o grupo diedral 5 (ver Exemplo 11, página 19).

Observemos que, sendo K_{11} um corpo finito, devemos ter $U(K_{11})$ cíclico de ordem 10, e portanto $U(K_{11}) \simeq C_{10}$.

Mostremos agora que, ao contrário de C_{10}, o grupo D_5 não é grupo multiplicativo de nenhum anel.

Para tal recordemos que, conforme vimos no Exemplo 11,

$$D_5 =< x, y \ ; \ x^5 = y^2 = 1 \text{ e } y^{-1}xy = x^{-1} > .$$

Notemos que, como $o(x) = 5$, temos $xy \neq yx$, pois do contrário deveríamos ter $x = x^{-1}$, o que seria um absurdo. Supondo R um anel tal que $U(R) \simeq D_5$, temos que existem $a, b \in U(R)$ tais que $U(R) =< a, b >$ onde $o(a) = 5$, $o(b) = 2$, $< a > \cap < b >= \{1\}$ e $b^{-1}ab = a^{-1}$.

Uma vez que $a \in C_{U(R)}(a)$, temos $< a > \subseteq C_{U(R)}(a)$, e daí, como $b \notin C_{U(R)}(a)$, temos $C_{U(R)}(a) =< a >= \{1, a, a^2, a^3, a^4\}$, uma vez que $5 \leq |C_{U(R)}(a)| < 10$ e $C_{U(R)}(a)$ é um subgrupo de $U(R)$.

Notemos também que $-1 \in C_{U(R)}(a)$ e assim $-1 = 1$, uma vez que do contrário teríamos $o(-1) = 2$, o que contrariaria o Teorema de Lagrange (vide Teorema 1, página 18), pois $|C_{U(R)}(a)| = 5$. Portanto, devemos ter $-1 = 1$ e assim $charR = 2$.

Consideremos $F = \{0, 1\} \subseteq R$ (observemos que F é um subanel de R e F é um corpo), e $p(x) = x^5 + 1$, $q(x) = x^2 + x + 1 \in F[x]$. Observemos que

$$p(x) = q(x)(x^3 + x^2 + 1) + x$$

e como $f(x) = x$ é irredutível e não divide $q(x)$ em $K[x]$, temos $f(x)$ e $q(x)$ são relativamente primos (vide Observação 13, página 34). Além disso, como $p(x) = q(x)(x^3 + x^2 + 1) + x$, devemos ter $p(x)$ e $q(x)$ relativamente primos. Daí, como $K[x]$ é um DFU tal que todos ideal é principal (vide Observação 15, página 36), existem $h(x)$ e $h_1(x) \in K[x]$, tais que $h(x)q(x) + h_1(x)p(x) = 1$. Assim, ao avaliarmos em a, iremos obter $q(a)h(a) = h(a)q(a) = 1$, uma vez

que $p(a) = 0$. Logo, como $q(a), h(a) \in R$, temos que $q(a) = a^2+a+1 \in U(R)$. Ademais, como $a(a^2+a+1) = (a^2+a+1)a$, temos que $a^2+a+1 \in C_{U(R)}(a)$. Assim, deve ocorrer alguma das possibilidades a seguir:

i)$a^2 + a + 1 = 1$, donde seguiria que $a^2 + a = 0$, ou seja $a^2 = a$, o que seria um absurdo.

ii)$a^2 + a + 1 = a$, e daí $a^2 + 1 = 0$ e portanto $a^2 = 1$, o que seria um absurdo, uma vez que $o(a) = 5$.

iii)$a^2 + a + 1 = a^2$, o que nos daria $a + 1 = 0$, ou seja, $a = 1$ o que seria um absurdo.

iv)$a^2+a+1 = a^3$, donde seguiria que $a^3+a^2+a = 1$ e portanto $a(a^2+a+1) = 1$, ou seja, $aa^3 = 1$. Mas isto seria um absurdo, uma vez que $o(a) = 5$.

v)$a^2 + a + 1 = a^4$, e daí $a^4 + a^2 + a = 1$ e portanto $a(a^3 + a^2 + 1) = 1$. Logo, $a^3 + a + 1 = a^{-1} = a^4 = a^2 + a + 1$, donde seguiria que $a^3 = a^2$, o que seria um absurdo.

Logo, como todas as possibilidades levam a um absurdo, concluímos que não existe anel R tal que $U(R) \simeq D_5$.

•Grupos de Ordem 11

Como podemos ver na Tabela 1.1, C_{11} é o único grupo de ordem 11, a menos de isomorfismo.

Notemos que C_{11} é um grupo abeliano finito, cuja ordem é um número primo e ímpar, e supondo R um anel tal que $U(R) = C_{11}$, pelo Corolário 2 devemos ter $|C_{11}| = 2^n - 1$, com $n \in \mathbb{N}$. Mas isto é um absurdo, uma vez que $|C_{11}| = 11$ e 11 não é da forma $2^n - 1$ para nenhum $n \in \mathbb{N}$. Logo, C_{11} não é grupo multiplicativo de nenhum anel.

Capítulo 3

Grupos Aditivos e Multiplicativos de Corpos

Neste capítulo estudaremos algumas condições necessárias para que um determinado grupo seja um grupo aditivo ou multiplicativo de um corpo e buscaremos determinar as propriedades intrínsecas dessas estruturas algébricas.

É importante destacar que como corpos são casos particulares de anéis todas os resultados obtidos no capítulo 2 continuam sendo válidos. Ademais, como as condições para que um anel seja um corpo são bastante exigentes, é de se esperar que os resultados obtidos sejam mais precisos e que estas estruturas sejam mais ricas em propriedades.

Neste capítulo, sendo K um corpo, iremos denotar o seu grupo multiplicativo $U(K)$ por K^*.

3.1 Grupos Aditivos de Corpos

Inicialmente iremos nos dedicar ao estudo da estrutura e das propriedades de grupos aditivos de corpos. Reforçamos aqui a ideia de que todos os resultados válidos para grupos aditivos de anéis continuam válidos no caso particular em que o anel em questão é um corpo. Entretanto, nessa seção iremos mostrar alguns resultados que valem especificamente para grupos aditivos de corpos.

Um fato conhecido é que o anel $\mathbb{Z}_n$ é um corpo se, e somente se, n é um número natural primo (vide Exemplo 27, página 31). Assim, o anel $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ não é um corpo, e observemos que embora $(\mathbb{Z}_6, +)$ seja um grupo de torção, pois é um grupo finito, $(\mathbb{Z}_6, +)$ não é um grupo de expoente primo, uma vez que $o(\overline{2}) = 3$ e $o(\overline{3}) = 2$. Mostremos agora que isto

não pode ocorrer em grupos aditivos de corpos. Para tal demonstremos o teorema a seguir.

Teorema 29. *Sendo K um corpo, então $(K,+)$ ou é livre de torção ou tem expoente primo.*

Demonstração. Por simplicidade de notação, denotaremos $(K,+)$ por G e por $T(G)$ o subgrupo de torção de $(K,+)$.

Iremos dividir a demonstração em dois casos $charK = 0$ e $charK \neq 0$.

Se $charK = 0$ e $x \in T(G)$, com $x \neq 0$, deve existir $n \in \mathbb{N}$ tal que $nx = 0$. Como $x \neq 0$, temos $x^{-1} \in K$ e portanto

$$n1 = n(xx^{-1}) = (nx)x^{-1} = 0$$

o que é um absurdo, pois $charK = 0$. Logo $T(G) = \{0\}$, e portanto G é livre de torção.

Se $charK \neq 0$, então $charK = p$, com $p \in \mathbb{N}$ e p primo (ver Teorema 10, página 36). Logo, devemos ter $px = 0$ para todo $x \in K$, sendo p mínimo nestas condições, e portanto $(K,+)$ tem expoente primo. □

Observemos que o Teorema 29 é válido independentemente de K ser finito ou infinito. Embora isso ocorra neste caso em particular, mostremos agora que algumas propriedades dos grupos aditivos de corpos dependem diretamente da finitude ou infinitude do corpo em questão.

Recordemos que sendo K um corpo finito, $(K,+)$ será um grupo finitamente gerado. O teorema a seguir irá garantir que tal propriedade não ocorre sob a hipótese de K ser um corpo infinito.

Teorema 30. *Seja K um corpo infinito. Então, $(K,+)$ não é finitamente gerado.*

Demonstração. Por simplicidade de notação, iremos denotar $(K,+)$ por G. Dividiremos a demonstração em dois casos, $charK = 0$ e $charK = p$, com p primo. Suponhamos inicialmente $charK = 0$, e neste caso podemos considerar que $\mathbb{Q}$ é o subcorpo primo de K. Assim, temos que $(\mathbb{Q},+) \leq G$ e, por simplicidade de notação, denotaremos $(\mathbb{Q},+)$ simplesmente por $\mathbb{Q}$.

Mostremos então que $\mathbb{Q}$ não é finitamente gerado. De fato, suponhamos, por absurdo, que $\mathbb{Q}$ seja finitamente gerado e tomemos $\frac{p_1}{q_1}, \frac{p_2}{q_2}, ..., \frac{p_n}{q_n} \in \mathbb{Q}$, com $q_i > 0$, tais que $< \frac{p_1}{q_1}, ..., \frac{p_n}{q_n} >= \mathbb{Q}$. Assim,

$$\mathbb{Q} = \left\{ k_1\frac{p_1}{q_1} + ... + k_n\frac{p_n}{q_n} \ / \ k_i \in \mathbb{Z} \right\}$$

e portanto deveriam existir $k_1, ..., k_n \in \mathbb{Z}$ tais que

$$\frac{1}{q_1 q_2 ... q_n + 1} = \frac{k_1 p_1}{q_1} + ... + \frac{k_n p_n}{q_n} = \frac{t}{q_1 q_2 ... q_n} \text{ , com } t \in \mathbb{Z}.$$

Logo,

$$q_1 ... q_n = t(q_1 ... q_n + 1)$$

o que é um absurdo, visto que $q_1 ... q_n + 1$ não divide $q_1 ... q_n$. Portanto, $\mathbb{Q}$ não é finitamente gerado e assim, pelo Teorema 2, temos G não finitamente gerado.

Suponhamos agora $charK = p$. Então, pelo Teorema 29, G é um grupo de expoente primo e portanto G é um grupo de torção. Assim, supondo G finitamente gerado, temos que G é um grupo abeliano finitamente gerado e de torção.

Tomando agora $g_1, ..., g_n \in G$ tais que $< g_1, ..., g_n >= G$, consideremos $H_i =< g_i >$ para cada $i \in \{1, 2, ..., n\}$. Assim, $G = H_1 + H_2 + ... + H_n$ e portanto G é finito, pois todos os $H_i's$ também o são, o que é um absurdo. Logo, G não pode ser finitamente gerado. □

Observemos agora que o Teorema 30 não vale para anéis em geral, uma vez que o anel dos inteiros $\mathbb{Z}$ é infinito, mas $(\mathbb{Z}, +)$ é cíclico e portanto finitamente gerado.

3.2 Grupos Multiplicativos de Corpos

Nesta seção iremos fazer um estudo análogo ao feito na Seção 3.1 voltado para grupos multiplicativos de corpos.

Inicialmente, observemos que se K é um subcorpo do corpo L, então seu grupo multiplicativo K^* é um subgrupo de L^*.

Como comentamos na Seção 3.1, o grupo aditivo de um corpo finito, sendo finito, é finitamente gerado. Mostremos agora que, mais que finitamente gerados, grupos multiplicativos de corpos finitos são na verdade cíclicos.

Sendo K um corpo finito, devemos ter $charK = p$, com p primo. Neste caso temos que $K_0 = \{0, 1_K, ..., (p-1)1_K\}$ é o subcorpo primo de K. Ademais, sendo K finito, temos que a extensão K/K_0 é finita.

Suponhamos então $m = [K : K_0]$ e $\beta = \{\alpha_1, ..., \alpha_m\}$ uma base de K sobre K_0, e consideremos a aplicação:

$$\begin{aligned} \varphi : \quad {K_0}^m &\longrightarrow K \\ (x_1, ..., x_m) &\longmapsto \varphi(x_1, ..., x_m) = x_1\alpha_1 + ... + x_m\alpha_m \end{aligned}$$

Como β é uma base de K sobre K_0, segue que todo elemento de K é uma combinação linear de elementos de β, e assim φ é uma função sobrejetiva. Supondo $(x_1, ..., x_m)$,$(y_1, ..., y_m) \in {K_0}^m$, tais que $\varphi(x_1, ..., x_m) = \varphi(y_1, ..., y_m)$ devemos ter

$$x_1\alpha_1 + ... + x_m\alpha_m = y_1\alpha_1 + ... + y_m\alpha_m$$

donde

$$(x_1 - y_1)\alpha_1 + ... + (x_m - y_m)\alpha_m = 0.$$

Como β é um conjunto LI, segue que $x_k - y_k = 0$, para todo $k \in \{1, ..., m\}$, ou seja, $x_k = y_k$, para todo $k \in \{1, ..., m\}$. Assim, φ é injetiva. Logo, φ é bijetora e portanto $|K| = |{K_0}^m| = |K_0|^m = p^m$. Daí, $|K^*| = p^m - 1$.

Além da informação que $|K^*| = p^m - 1$, para mostrar que o grupo multiplicativo de um corpo finito é cíclico, necessitamos ainda dos seguintes lemas.

Lema 4. *Se K é um corpo, então para cada $n \in \mathbb{N}$ a equação $x^n = 1$ tem no máximo n soluções em K^*.*

Demonstração. Basta considerar o polinômio $f(x) = x^n - 1 \in K[x]$ e observar que um polinômio de grau n sobre o corpo K, tem no máximo n soluções em K. □

Lema 5. *Sejam G um grupo abeliano finito e $k = max\{o(g) \ / \ g \in G\}$. Então $o(g)$ divide k, para todo $g \in G$.*

Demonstração. Consideremos $x_0 \in G$ tal que $o(x_0) = k$ e suponhamos, por contradição, que existe $g \in G$ tal que $o(g)$ não divide k. Então, existem $r, s, p \in \mathbb{N}$, p primo, tais que $k = rp^n$ e $o(g) = sp^m$, com $0 \leq n < m$ e $mdc(r, p) = mdc(s, p) = 1$. Tomando agora $a = (x_0)^{p^n}$ e $b = g^s$, temos $o(a) = r$ e $o(b) = p^m$. Como $ab = ba$ e $mdc(o(a), o(b)) = 1$, temos $o(ab) = o(a)o(b) = rp^m > k$, o que é um absurdo.

Portanto, $o(g)$ divide k, para todo $g \in G$. □

Mostremos então que, de fato, o grupo multiplicativo de um corpo finito é cíclico.

Teorema 31. *Seja K um corpo finito. Então, K^* é cíclico.*

Demonstração. Pelo Lema 4, temos que para cada $n \in \mathbb{N}$ a equação $x^n = 1$ tem no máximo n soluções em K^*. Em particular, para $k = max\{o(x) \ / \ x \in K^*\}$ a equação $x^k = 1$ deve ter no máximo k soluções em K^*.

Supondo, por contradição, que K^* não é cíclico, devemos ter $k < |K^*|$. Entretanto, pelo Lema 5, temos que $o(x)$ divide k, donde $x^k = 1$, para todo $x \in K^*$. Daí, a equação $x^k = 1$ tem $|K^*|$ soluções em K^*. Mas $|K^*| > k$, o que é um absurdo. Portanto, K^* é cíclico. □

Recordemos que no Teorema 30 garantimos que o grupo aditivo de um corpo infinito não é finitamente gerado. Mostremos agora que vale um resultado análogo para grupos multiplicativos de corpos infinitos.

Para tal consideremos D um DFU e K_D seu corpo de frações. Consideremos também P um conjunto completo e não redundante de elementos irredutíveis de D, isto é, todo elemento irredutível de D é associado a algum elemento de P e os elementos de P são, dois a dois, não associados.

Suponhamos P infinito e definamos

$$G = \{f : P \longrightarrow \mathbb{Z} \; ; f \text{ é quase nula}\}.$$

Recordemos que, G munido da operação de adição ponto a ponto, é um grupo abeliano (ver Exemplo 8, página 18).

Consideremos agora a aplicação $\varphi : U(D) \times G \longrightarrow {K_D}^*$, definida por $\varphi(u, f) = u \prod_{p \in P} p^{f(p)}$. Inicialmente observemos que, da forma como G foi definido, $\prod_{p \in P} p^{f(p)}$ é sempre um produto finito e, como todos os termos são não nulos temos $\varphi(u, f) \in {K_D}^*$, para todo $(u, f) \in U(D) \times G$. Assim, φ está bem definida. Notemos agora que φ é um homomorfismo de grupos. De fato, dados $(u, f), (v, g) \in U(D) \times G$, temos

$$\begin{aligned}
\varphi(uv, f+g) &= uv \prod_{p \in P} p^{(f+g)(p)} \\
&= uv \prod_{p \in P} p^{f(p)+g(p)} \\
&= uv \prod_{p \in P} p^{f(p)} p^{g(p)} \\
&= \left(u \prod_{p \in P} p^{f(p)} \right) \left(v \prod_{p \in P} p^{g(p)} \right) \\
&= \varphi(u, f)\varphi(v, g)
\end{aligned}$$

Ademais, dado $k \in {K_D}^*$ temos $k = \frac{a}{b}$, com $a, b \in D - \{0\}$, e como D é um DFU, temos $a = u{p_1}^{n_1}{p_2}^{n_2}...{p_s}^{n_s}$ e $b = v{p_1}^{m_1}{p_2}^{m_2}...{p_s}^{m_s}$ com $p_1, ..., p_s \in P$, $u, v \in U(D)$ e $m_1, ..., m_s$ inteiros não negativos. Assim,

$$k = \frac{a}{b} = uv^{-1}{p_1}^{n_1 - m_1}...{p_s}^{n_s - m_s}$$

com $uv^{-1} \in U(D)$, e daí concluímos que φ é sobrejetiva.

Observemos agora que $Ker\ \varphi = \{(u, f) \in U(D) \times G \ / \ \varphi(u, f) = 1\}$. Assim, se $(u, f) \in Ker\ \varphi$, temos

$$1 = \varphi(u, f) = u \prod_{p \in P} p^{f(p)} = u{p_{n_1}}^{k_1} ... {p_{n_s}}^{k_s}$$

e daí

$${p_{n_1}}^{|k_1|} ... {p_{n_s}}^{|k_s|} = u{p_{n_1}}^{k_1+|k_1|} ... {p_{n_s}}^{k_s+|k_s|} \ .$$

Como $k_i + |k_i| \geq 0$ e D é um DFU, pela unicidade da decomposição, devemos ter $u = 1$ e $k_i + |k_i| = k_i$, para todo $i = 1, 2, ..., s$. Logo, $k_i = 0$, para todo $i = 1, ..., s$, donde concluímos que φ é injetiva. Assim, φ é um isomorfismo de grupos.

Recordemos agora que isomorfismos preservam conjuntos geradores (vide Proposição 2, página 23). Assim, supondo ${K_D}^*$ finitamente gerado, deveríamos ter $U(D) \times G$ também finitamente gerado.

Por outro lado, sendo $U(D) \times G$ finitamente gerado, G também o seria. Mas, supondo $\{f_1, f_2, ..., f_n\}$ um conjunto gerador de G e destacando $P_0 = \{p_j \ / \ j \in \mathbb{N}\} \subset P$ um subconjunto enumerável, como cada $f_i \in G$, existem $p_{t_1}, p_{t_2}, ..., p_{t_n} \in P_0$ tais que $f_i(p_j) = 0$ sempre que $j > t_i$. Tomando agora $t = max\{t_1, ..., t_n\}$, definamos a função $f : P \longrightarrow \mathbb{Z}$, dada por:

$$f(p) = \begin{cases} 1 & , \text{ se } p = p_{t+1} \\ 0 & , \text{ se } p \in P - \{p_{t+1}\} \end{cases}$$

Temos $f \in G$, mas $f \notin < f_1, f_2, ..., f_n >$, o que é um absurdo. Logo, K^* não é finitamente gerado e temos o seguinte resultado:

Proposição 6. *Sejam D um DFU e K_D seu corpo de frações. Consideremos P um conjunto completo e não redundante de elementos irredutíveis de D. Se P é infinito, então ${K_D}^*$ não é finitamente gerado.*

Após essas considerações, mostremos de fato que K^* não é finitamente gerado quando K é um corpo infinito.

Teorema 32. *Sejam K um corpo infinito e K^* seu grupo multiplicativo. Então, K^* não é finitamente gerado.*

Demonstração. Dividiremos a demonstração em dois casos: $charK = 0$ e $charK = p$, com p primo. Suponhamos então $charK = 0$. Neste caso podemos considerar que $\mathbb{Q}^* \leq K^*$. Mostremos então que $\mathbb{Q}^*$ não é finitamente gerado. Para tal, observemos que $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$ e que considerando P como o conjunto dos números primos positivos, temos que P é um conjunto completo, não redundante e infinito de elementos irredutíveis de $\mathbb{Z}$. Logo, pela Proposição 6, segue que $\mathbb{Q}^*$ não é finitamente gerado. Portanto,

K^* não é finitamente gerado, uma vez que $\mathbb{Q}^* \leq K^*$ (vide Teorema 2, página 20).

Mostremos agora o resultado no caso em que $charK = p$. Neste caso (vide Exemplo 30, página 36), temos que existe K_0 subcorpo de K tal que $|K_0| = p$ ($K_0 = \{0, 1_K, ..., (p-1)1_K\}$) e consideremos a extensão K/K_0.

Suponhamos que K^* é finitamente gerado, digamos $K^* =< a_1, ..., a_n >$. Observa-se que neste caso, $K = K_0(a_1, ..., a_n)$. Notemos que se a extensão K/K_0 é algébrica, como K_0 é finito e a extensão K/K_0 é finitamente gerada e algébrica, devemos ter K/K_0 finita (vide Seção 1.3.2, página 37) e portanto K finito, o que é uma contradição. Assim, a extensão K/K_0 deve ser transcendente.

Sendo K/K_0 uma extensão transcendente, tomemos $a \in K$ um elemento transcendente sobre K_0. Nesta situação, recordemos que conforme comentamos na Seção 1.3.2, temos $K_0[a] \simeq K_0[x]$, e portanto $K_0(a) \simeq K_0(x)$, onde $K_0(a)$ e $K_0(x)$ denotam os corpos de frações de $K_0[a]$ e $K_0[x]$, respectivamente.

Recordemos que se L é um corpo finito, então para todo $n \in \mathbb{N}$ existe algum polinômio de grau n irredutível em $L[x]$ (ver Observação 15, página 36). Assim, como K_0 é um subcorpo finito de K, qualquer conjunto completo não redundante de elementos irredutíveis de $K_0[x]$ deve ser infinito, pois para cada número natural n existe um polinômio de grau n irredutível em $K_0[x]$. Então $K_0[x]$ é um DFU que possui um conjunto completo, não redundante e infinito de elementos irredutíveis, e daí, pela Proposição 6, $K_0(x)$, que é seu corpo de frações, é tal que $K_0(x)^*$ não é finitamente gerado.

Portanto, como $K_0(a)^* \simeq K_0(x)^*$, uma vez que $K_0(a) \simeq K_0(x)$, temos que $K_0(a)^*$ não é finitamente gerado. Logo, de $K_0(a)^* \leq K^*$ e do Teorema 2 decorre que K^* não é finitamente gerado. □

Observemos agora que, conforme ocorreu com o Teorema 30, o Teorema 32 também não é válido para grupos multiplicativos de anéis em geral. De fato, na Seção 2.2.3 mostramos que $A = \left\{ \frac{f(x)}{x^n} / f(x) \in K[x] \text{ e } n \in \mathbb{N} \right\}$ onde $K = \{0, 1\}$ é um anel cujo grupo multiplicativo é infinito, embora $U(A)$ seja cíclico e portanto finitamente gerado.

3.3 Relação entre $(K, +)$ e K^*

Neste ponto é importante destacar que embora os grupos aditivos e multiplicativos de corpos tenham características algébricas em comum, conforme mostram os Teoremas 30 e 32, em suas essências essas estruturas algébricas

são diferentes, no sentido de que sendo K um corpo não existe um isomorfismo entre $(K,+)$ e K^*, conforme garante o teorema a seguir.

Este fato é facilmente observável no caso de corpos finitos, pois nesse caso os grupos aditivos e multiplicativos têm ordens diferentes, garantindo assim o resultado.

Apresentaremos agora uma demonstração para o caso mais geral em que K é um corpo infinito.

Teorema 33. *Seja K um corpo. Então, $(K,+)$ e K^* não são isomorfos.*

Demonstração. Suponha que $\varphi : (K,+) \longrightarrow K^*$ seja um isomorfismo, isto é, φ é bijetora e $\varphi(x+y) = \varphi(x)\varphi(y)$, para quaisquer $x, y \in (K,+)$.

Sendo $x \in (K,+)$ tal que $2x = x + x = 0$, então $h = \varphi(x) \in K^*$, devemos ter

$$1 = \varphi(0) = \varphi(x+x) = \varphi(x)\varphi(x) = h^2.$$

Assim, para cada $x \in (K,+)$ tal que $2x = 0$, existe $h \in K^*$ tal que $h^2 = 1$, a saber, $h = \varphi(x)$. Além disso, φ^{-1} é também um isomorfismo e daí essa correspondência é biunívoca. Logo, a quantidade de soluções da equação $2x = 0$ em $(K,+)$ é igual à quantidade de soluções da equação $x^2 = 1$ em K^*.

Se $charK = 2$, temos $-1 = 1$ e assim o número de soluções da equação $x^2 = 1$ em K^* é igual a 1. Mas, como $charK = 2$, todo elemento de $(K,+)$ é solução da equação $2x = 0$, o que é uma contradição, pois as quantidades de soluções das duas equações anteriores deveriam coincidir.

Se $charK \neq 2$, então a equação $x^2 = 1$ tem exatamente duas soluções em K^*, a saber $x = 1$ e $x = -1$, enquanto a equação $2x = 0$ admite apenas uma solução $(x = 0)$ em $(K,+)$, o que é uma contradição.

Logo, $(K,+)$ e K^* não são isomorfos. □

Observemos que a demonstração apresentada também garante a validade do Teorema 33 para domínios de integridade.

Apresentaremos agora um exemplo garantindo que este resultado não é válido para anéis quaisquer de característica 2.

Exemplo 31. *Consideremos o corpo $K = \{0,1\}$ e V um K-espaço vetorial com base $\beta = \{v_1, v_2, v_3, ...\}$. Para cada $n \in \mathbb{N}$, definamos $E_n : V \to V$ como sendo o operador linear tal que*

$$E_n(v_j) = \begin{cases} v_{2n} & , \text{ se } j = 2n-1 \\ 0 & , \text{ caso contrário} \end{cases}$$

Temos que $E_n E_m = 0$ para quaisquer $n, m \in \mathbb{N}$.

Consideremos agora W o subespaço de $\mathcal{L}(V)$ (vide Exemplo 19, página 27) gerado por $\{E_n \ / \ n \in \mathbb{N}\}$, e observemos que, como $E_nE_m = 0$ para quaisquer $n, m \in \mathbb{N}$, se $T, S \in W$, então $TS = 0$.

Tomemos agora o subespaço $R = W_1 + W$ de $\mathcal{L}(V)$, onde W_1 é o subespaço de $\mathcal{L}(V)$ gerado pelo operador identidade I de V. Dados $T, S \in R$, temos $T = \lambda_1 I + F_1$ e $S = \lambda_2 I + F_2$ com $\lambda_1, \lambda_2 \in K$ e $F_1, F_2 \in W$. Daí,

$$T + S = \lambda_1 I + F_1 + \lambda_2 I + F_2 = (\lambda_1 + \lambda_2)I + (F_1 + F_2) \in R$$

e

$$TS = (\lambda_1 I + F_1)(\lambda_2 I + F_2) = \lambda_1\lambda_2 I + \lambda_2 F_1 + \lambda_1 F_2 \in R$$

pois $F_1F_2 = 0$. Assim, R é um subanel de $\mathcal{L}(V)$ e $I \in R$. E observemos que se $T \in W$, então $TT = 0$ e supondo $T \in GL(V)$ teríamos

$$T = IT = T^{-1}TT = T^{-1}0 = 0$$

o que seria um absurdo. Logo $T \notin GL(V)$. Ademais, temos

$$\begin{aligned} (I + T)(I - T) &= I + TI - IT - TT \\ &= I + TI - TI - TT \\ &= I \end{aligned}$$

uma vez que $TT = 0$. Logo, $U(R) = \{I + T \ / \ T \in W\}$.

Agora consideremos a aplicação $f : (W, +) \longrightarrow U(R)$ que é definida por $f(T) = I + T$. Notemos que dados $T, S \in W$ temos

$$\begin{aligned} f(S + T) &= I + S + T \\ &= I + SI + IT + ST \\ &= (I + S)(I + T) \\ &= f(S)f(T) \end{aligned}$$

Logo, f é um homomorfismo de grupos e como $U(R) = \{I + T \ ; T \in W\}$, segue que f é sobrejetivo. Ademais, se $f(S) = f(T)$, então $I + S = I + T$ e daí $S = T$. Portanto, f é um isomorfismo de grupos e assim $U(R) \simeq (W, +)$.

Mostremos agora que $(R, +) \simeq (W, +)$. Para tal consideremos a base $\gamma = \{E_n \ ; n \in \mathbb{N}\}$ de W, a base $\beta = \{I\} \cup \gamma$ de R e a transformação linear $T : R \longrightarrow W$ tal que $T(I) = E_1$ e $T(E_n) = E_{n+1}$. Claramente temos T um isomorfismo de espaços vetoriais. Daí, R e W são isomorfos como espaços vetoriais e portanto como grupos aditivos. Logo, $U(R) \simeq (W, +) \simeq (R, +)$ e portanto $U(R) \simeq (R, +)$

Assim, concluímos que o Teorema 33 apresentado não é válido em geral para anéis de característica 2.

Embora o Teorema 33 nos garanta que dado um corpo K, temos $(K,+) \ncong K^*$, apresentaremos agora um exemplo, onde ocorre $(K,+) \simeq H$, onde H é um subgrupo de K^*.

Exemplo 32. *Observando que* $\mathbb{R}_+ = \{x \in \mathbb{R} \ / \ x > 0\}$ *é um subgrupo de* $\mathbb{R}^*$, *consideremos a aplicação*

$$\begin{aligned} f : (\mathbb{R},+) &\longrightarrow {\mathbb{R}^*}_+ \\ x &\longmapsto f(x) = \ln x \end{aligned}$$

e observemos que dados $x, y \in (\mathbb{R},+)$, *temos*

$$f(x+y) = \ln(x+y) = (\ln x)(\ln y) = f(x)f(y).$$

Assim, f *é um homomorfismo de grupos. Além disso, uma vez que vale* $\ln x = \ln y$ *se, e somente se,* $x = y$, *temos* f *injetiva. Ademais, claramente* f *é sobrejetiva e assim* $(\mathbb{R},+) \simeq {\mathbb{R}^*}_+$.

Para finalizarmos esta seção, demonstraremos que sendo K um corpo, embora $(K,+)$ e K^* não sejam isomorfos, existe uma relação entre $(K,+)$ e K^*. Esta relação é dada pelo teorema a seguir.

Teorema 34. *Seja* F *um corpo. Então,* F^* *é isomorfo a algum subgrupo de* $Aut\ (F,+)$.

Demonstração. Inicialmente observemos que dado $a \in F^*$, a função

$$\begin{aligned} f_a : (F,+) &\longrightarrow (F,+) \\ x &\longmapsto f_a(x) = ax \end{aligned}$$

é um homomorfismo de grupos. De fato, dados $x, y \in F$, temos

$$f_a(x+y) = a(x+y) = ax + ay = f_a(x) + f_a(y).$$

Além disso, dado $x \in F$, tomemos $y = a^{-1}x \in F$ e daí

$$f_a(y) = ay = aa^{-1}x = x.$$

Logo, f_a é sobrejetiva. Ademais, pela Lei do Cancelamento (vide Observação 1, página 14), temos f_a injetiva. Portanto f_a é um automorfismo de $(F,+)$ para todo $a \in F^*$.

Consideremos agora a seguinte aplicação

$$\begin{aligned} f : F^* &\longrightarrow Aut\ (F,+) \\ a &\longmapsto f(a) = f_a \end{aligned}$$

e observemos que, como $f_a \in Aut\ (F,+)$, f está bem definida. Ademais, f é um homomorfismo de grupos. De fato, dados $a, b \in F^*$ e $x \in F$, temos

$$f_{ab}(x) = abx = af_b(x) = f_a(f_b(x)) = (f_a \circ f_b)(x).$$

Logo, $f(ab) = f_{ab} = f_a \circ f_b = f(a)f(b)$, para todos $a, b \in F^*$. Além disso, observemos que $Ker\ f = \{a \in F^*\ /\ f_a = I\}$, onde I denota a aplicação identidade de $(F,+)$. Assim, se $a \in Ker\ f$, então particularmente temos $1_F = f_a(1_F) = a1_F$, donde $a = 1_F$. Portanto, $Ker\ f = \{1_F\}$ e daí f é um homomorfismo injetivo de grupos. Logo, pelo Teorema Fundamental dos Homomorfismos (vide Teorema 4, página 33), temos $F^* \simeq Imf$, que é um subgrupo de $Aut(F,+)$. □

Conforme demonstramos no Teorema 33, sendo K um corpo, devemos ter $(K,+) \ncong K^*$. Portanto, devem existir algumas características destoantes entre essas estruturas algébricas.

A título de ilustração, apresentaremos uma dessas características na seção a seguir.

3.3.1 Torção em Grupos Multiplicativos de Corpos

Nesta seção iremos estudar torção em grupos multiplicativos de corpos. Inicialmente, observemos que se K é um corpo, então 1_K e -1_K são elementos de torção em K, valendo a ressalva de que se $charK = 2$, então $-1_K = 1_K$. Mostraremos no decorrer desta seção que existem corpos onde esses elementos são os únicos elementos de torção.

Observemos também que se K é um corpo finito, então K^* é finito e portanto de torção. Mostremos agora que o mesmo pode não ocorrer para K^* se K é um corpo infinito.

Exemplo 33. *Consideremos $K = \{0,1\}$ um corpo de dois elementos e consideremos o corpo de frações $K(x)$ do anel $K[x]$. Recordemos que apresentamos $K(x)$ na Seção 2.2.3 e na Seção 3.2 mostramos o Teorema 6, que nos garante que $U(K(x)) \simeq U(K[x]) \times G$, onde $G = \{f : P \longrightarrow \mathbb{Z}\ /\ f$ é quase nula$\}$ e P é um conjunto completo e não redundante de irredutíveis de $K[x]$. Mostremos agora que $U(K(x))$ é livre de torção.*

Inicialmente, notemos que como $K = \{0,1\}$ e os elementos inversíveis de $K[x]$ são os polinômios constantes não nulos (conforme visto na Observação

15, página 36), temos $U(K[x]) = \{1\}$ e portanto $U(K(x)) \simeq G$. Então, para mostrarmos que $U(K(x))$ é livre de torção, necessitamos apenas mostrar que G é livre de torção. Suponhamos então $f \in G$ tal que $f \not\equiv 0$ e seja um elemento de torção. Assim, existe $m \in \mathbb{N}$ tal que $mf \equiv 0$. Mas isto é um absurdo, uma vez que, como $f \not\equiv 0$, existe $p \in P$ tal que $f(p) = k \neq 0$ e daí $(mf)(p) = mf(p) = mk \neq 0$. Logo, G é livre de torção e portanto $U(K(x))$ é livre de torção.

Recordemos que no Teorema 29 garantimos que o grupo aditivo de um corpo ou tem expoente primo ou é livre de torção. Mostraremos mais adiante que o mesmo não ocorre para grupos multiplicativos de corpos em geral.

Relembremos agora o conceito de corpo ordenado.

Definição 44. Seja K um corpo. Dizemos que K é um corpo ordenado quando existe $P \subset K$, chamado de conjunto dos elementos positivos de K, tal que as seguintes condições são satisfeitas:

P1. A soma e o produto de elementos positivos são positivos, isto é, se $x, y \in P$, então $x + y \in P$ e $xy \in P$;

P2. Dado $x \in P$, ocorre exatamente uma das seguintes alternativas: $x = 0$, $x \in P$ ou $-x \in P$.

Sendo K um corpo ordenado, definimos uma relação de ordem em K da seguinte forma: dados $x, y \in K$, dizemos que x é *menor ou igual* a y, e denotamos por $x \leq y$, quando $y - x \in P \cup \{0\}$. Ademais, a relação "$\leq$" definida desta maneira é um relação de ordem total em K e é facilmente observável que $P = \{x \in K \ / \ 0 < x\}$ (observando que $x < y$ significa $x \leq y$ e $x \neq y$).

Observação 17. *Seja K um corpo ordenado.*

i) Se $x \in K^*$, então $(-x)^2 = x^2 \neq 0$ e assim $x^2 \in P$. Particularmente, $1_K \in P$;

ii) Se $x \in P$, então $x^{-1} \in P$. De fato, se $x^{-1} \notin P$, teríamos $-x^{-1} \in P$ e daí $-1_K = x(-x^{-1}) \in P$, um absurdo;

iii) $P \leq K^*$.

Pelo que vimos P é um subgrupo de K^*. Vejamos agora que P é um grupo livre de torção. De fato, seja $a \in P$ e suponhamos a um elemento de torção. Assim, existe $n \in \mathbb{N}$ tal que $a^n = 1$ e logo devemos ter

$$0 = a^n - 1 = (a - 1)(a^n + a^{n-1} + ... + a + 1).$$

Como $a > 0$, concluímos que $a^n + a^{n+1} + ... + a + 1 > 0$, e portanto $a - 1 = 0$, ou seja, $a = 1$. Logo, P é um grupo livre de torção, como afirmado.

Observemos também que se $CharK = p$, com p primo, então

$$p1 = \underbrace{1 + 1 + ... + 1}_{p \ parcelas} = 0.$$

Logo, K não pode ser ordenado, pois caso fosse deveríamos ter $1 > 0$ e daí $p1$ também o seria. Portanto, sendo K um corpo ordenado devemos ter $CharK = 0$.

Uma outra informação importante a respeito do conjunto P, como definido anteriormente, é que considerando o produto direto $\{-1_K, 1_K\}$ e a aplicação

$$\begin{aligned} f : \{-1_K, 1_K\} \times P &\longrightarrow K^* \\ (a, x) &\longmapsto f(a, x) = ax \end{aligned}$$

observa-se facilmente que f é um homomorfismo injetivo de grupos, e da propriedade P2 na Definição 44 segue que f é sobrejetivo. Assim, temos $K^* \simeq \{-1_K, 1_K\} \times P$.

Agora, após essas considerações, passemos ao resultado.

Teorema 35. *Seja K um corpo ordenado. Então, $|T(K^*)| = 2$ e ainda $T(K^*) = \{-1_K, 1_K\}$, onde $T(K^*)$ denota o subgrupo de torção de K^**

Demonstração. Sendo K um corpo ordenado, conforme comentamos anteriormente $K^* \simeq \{-1_K, 1_K\} \times P$, onde P é o conjunto dos elementos positivos de K. Assim, uma vez que P é um grupo livre de torção, temos que $T(K^*) = \{-1_K, 1_K\}$. □

Observemos que a recíproca do teorema acima não é válida, pois ao considerarmos $K_3 = \{0, 1, 2\}$ (corpo de 3 elementos), temos

$$T(K_3^*) = K_3^* = \{1, 2\} = \{-1, 1\},$$

mas K_3 tem característica 3 e portanto não é ordenável.

Na verdade, se K^* é um grupo de expoente finito, então K^* é um grupo finito. De fato, se K é infinito, então ao supormos K^* de expoente finito deveríamos ter $k^n = 1$ para todo $k \in K^*$, para algum $n \in \mathbb{Z}$. Assim, o polinômio $f(x) = x^n - 1 \in K[x]$ iria possuir infinitas soluções em K, o que seria um absurdo. Logo, se K é infinito, então K^* não tem expoente finito.

Segue ainda que se K^* é um grupo de expoente primo, então K é o corpo de 3 elementos. De fato, se K^* é um grupo de expoente primo, então, conforme comentamos anteriormente, K é finito, digamos $|K| = p^m$, e daí, pelo Teorema 31, devemos ter $K^* =< a >$ e $|K^*| = o(a) = p^{m-1}$. Sendo K^*

cíclico finito, temos $exp\ K^* = |K^*|$ e assim $|K^*|$ deve ser um número primo por hipótese. Entretanto, p^{m-1} é primo apenas quando $p = 3$ e $m - 1 = 1$, ou seja, quando $|K| = 3$. Logo, K^* é um grupo de expoente primo, apenas quando K é o corpo de 3 elementos.

Para finalizarmos este capítulo, iremos utilizar alguns conceitos básicos da teoria de extensões de corpos para caracterizar corpos cujos grupos multiplicativos são grupos de torção.

Entretanto, antes de exibirmos a caracterização, será necessário apresentarmos um resultado auxiliar.

Lema 6. *Seja K um corpo tal que K^* é um grupo de torção. Então, $charK = p$, com p primo.*

Demonstração. Inicialmente, recordemos que, se K é um corpo, então temos $charK = 0$ ou $charK = p$ (ver Teorema 10). Suponhamos, por contradição, $charK = 0$. Então podemos considerar $\mathbb{Q} \subseteq K$, e consequentemente $\mathbb{Q}^* \leq K^*$.

Assim, como K^* é um grupo de torção, deveríamos ter $\mathbb{Q}^*$ sendo um grupo de torção, o que seria um absurdo, pois $2 \in \mathbb{Q}^*$ e $2^n \neq 1$, para todo $n \in \mathbb{N}$. Logo, $charK \neq 0$, e portanto $charK = p$, com p primo. □

Agora passemos à caracterização.

Teorema 36. *Se K é um subcorpo do fecho algébrico do $\mathbb{Z}_p$, com p primo, então K^* é um grupo de torção. Reciprocamente, se K é um corpo tal que K^* é um grupo de torção, então K está imerso no fecho algébrico de $\mathbb{Z}_p$.*

Demonstração. Seja $a \in K^*$. Então, como $K \subset \overline{\mathbb{Z}_p}$, temos a algébrico sobre $\mathbb{Z}_p$. Assim, o corpo $\mathbb{Z}_p(a)$ é uma extensão simples e algébrica de $\mathbb{Z}_p$, e portanto segue do Teorema 16 que $\mathbb{Z}_p(a)$ é uma extensão finita de $\mathbb{Z}_p$. Ademais, uma vez que $\mathbb{Z}_p$ é um corpo finito, temos que $\mathbb{Z}_p(a)$ é um corpo finito, e portanto $o(a)$ é finita (pois, $a^m = 1$, com $m = |\mathbb{Z}_p(a)| - 1$), ou seja, $a \in T(K^*)$. Pela arbitrariedade de $a \in K^*$, concluímos que K^* é um grupo de torção.

Reciprocamente, se K é um corpo tal que K^* é um grupo de torção, pelo Lema 6, devemos ter $charK = p$ e assim existe F subcorpo de K com $\mathbb{Z}_p \simeq F$. Ademais, tomando arbitrariamente $a \in K^*$, existe $n \in \mathbb{N}$ tal que $a^n = 1$, e assim a é raiz do polinômio $f(x) = x^n - 1 \in F[x]$.

Da arbitrariedade de a segue que K é uma extensão algébrica de F. Logo, pelo Teorema da Extensão do Isomorfismo (ver Teorema 12), devemos ter K imerso no fecho algébrico de $F \simeq \mathbb{Z}_p$, o que conclui a demonstração, uma vez que $\mathbb{Z}_p \simeq F$.

□

Referências Bibliográficas

[1] ATIYAH, M. F, MACDONALD, I. G. *Introduction to Commutative Algebra*. New York: Addsion-Wesley, 1969.

[2] DITOR, S. Z. *On the Group of Units of a Ring*. The American Mathematical Monthly. 78(5), 522-523, 1971.

[3] ENDLER, O. *Teoria dos Corpos*. Rio de Janeiro: IMPA, 2009.

[4] FRALEIGH, J. B. *A First Course in Abstract Algebra*. 6ª Edição. New York: Addison-Wesley, 2000.

[5] GARCIA, A, LEQUAIN, Y. *Elementos de Álgebra*. 5ª Edição. Rio de Janeiro: Projeto Euclides, IMPA, 1999.

[6] GONÇALVES, A. *Introdução à Álgebra*. 2ª Edição. Rio de Janeiro: Projeto Euclides, IMPA, 2003.

[7] HEFEZ, A. *Elementos de Aritmética*. 2ª Edição. Rio de Janeiro: SBM, 2011.

[8] HOFFMAN, K, KUNZE, R. *Álgebra linear*. 2ª Edição Trad. Rio de Janeiro: LTC, 1979.

[9] LIMA, E. L. *Curso de Análise*. 13ª Edição. Rio de Janeiro, Brasil: IMPA, 2011.

[10] MARTIN, P. A. *Grupos, Corpos e Teoria de Galois*. São Paulo: Editora Livraria da Física, 2010.

[11] ROTMAN, J. J. *An Introduction to the Theory of Groups*. 4ª Edição. New York: Springer-Verlog, 1994.

[12] VIEIRA, V. L. *Álgebra Abstrata para Licenciatura*. Campina Grande: EDUEPB, 2013.